이스트시큐리티

보안 동향 보고서

No.146 2021.11

No.146 2021.11

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 06-12

지속적으로 유포중인 국민비서 사칭 스팸메일 주의!

北 평양과학기술대학 총장을 사칭한 CVE-2021-40444 취약점 공격 주의

03 악성코드 분석 보고 13-15

04 글로벌 보안 동향 16-23

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2021 년 10 월에는 개인 정보 유출 사건이 유독 많이 발생하였습니다.

국내 최대 이커머스 업체 쿠팡에서 모바일 어플리케이션 첫 화면에 본인 정보가 아닌 다른 회원의 이름과 주소 등 약 30 만명의 개인정보가 1 시간 동안 노출되었습니다. 또한 데이팅 애플리케이션 골드스푼도 내부 정보망에서 해킹 흔적이 발견되었고 회원아이디, 이름, 생년월일, 전화번호, 회원들이 제출한 자료 등 13 만명의 개인정보가 유출되었습니다. 마지막으로 패션 커머스 플랫폼 브랜디의 고객 데이터베이스 해킹으로 인해 700 만명의 회원아이디, 패스워드, 이메일 주소 등을 판매하는 게시글이 딥웹에 올라오기도 하였습니다.

랜섬웨어와 비트코인 탈취로 유명한 라자루스(Lazarus)그룹이 IT 공급망을 공격하기 시작했습니다.
공격 대상은 한국의 보안 소프트웨어 벤더사와 라트리비아에 있는 IT 자산관리제품 판매업체로 확인되었으며 한국의 한 싱크탱크 조직에 원격 접근 트로이목마인 블라인딩캔(Blindingcan)과 코퍼헤지(Copperhedge)를 사용한것으로 확인되었습니다. 사용된 악성코드는 감염된 기기의 정보와 내부 파일 검색 및 전송 등 시스템을 장악하기보다는 감염 시스템의 정보를 수집하기 위해 사용되었습니다. 라자루스 그룹이 지속적인 IT 업체를 공격하는 것은 앞으로도 지속적인 IT 공급망을 장악하기 위함으로 판단할 수 있습니다.

북한 배후로 추정되는 탈륨 (Thallium) (또는 김수키(Kimsuky)라고도 부름) 조직은 ““중요한 미팅” 장인 노태우 조문하고 미국 가는 최태원”이라는 제목의 스피어 피싱 악성 메일을 유포하였습니다. 이는 시사 정치 뉴스처럼 가장해 본문의 URL 링크를 클릭하면 실제 기사화되었던 뉴스 내용을 무단 인용한 허위 사이트가 보여지며 사용자의 IP 주소 및 웹브라우저등 개인 정보가 수집됩니다.

악성코드 및 해킹 공격들은 점점 정교화 되고 사회공학적 수법들을 사용하면서 위협성 역시 증가하고 있습니다. 특히 개인 정보가 유출되면, 부정 결제나 대출 등의 2 차 피해를 입을 수 있기 때문에 메일이나 문자메시지, SNS 로 오는 URL 들에 대해서 각별한 주의가 요구되고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021 년 10 월의 감염 악성코드 Top 15 리스트에서는 Worm.ACAD.Bursted 악성코드가 1 위로 새롭게 진입하였고, 지난달에 1 위를 차지했던 Gen:Variant.Razy.767621 은 2 계단 하락하였다. 이번 달에는 지난달과 비교하여 디자인 소프트웨어 오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted 와 실행 파일을 감염시키는 Win32.Floxif.Dam 악성코드가 새롭게 진입하였고, Trojan.ShadowBrokers.A 가 10 계단 하락하여 12 위를 기록했다. 10 월에는 Worm.ACAD.Bursted 을 비롯하여 3 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다.

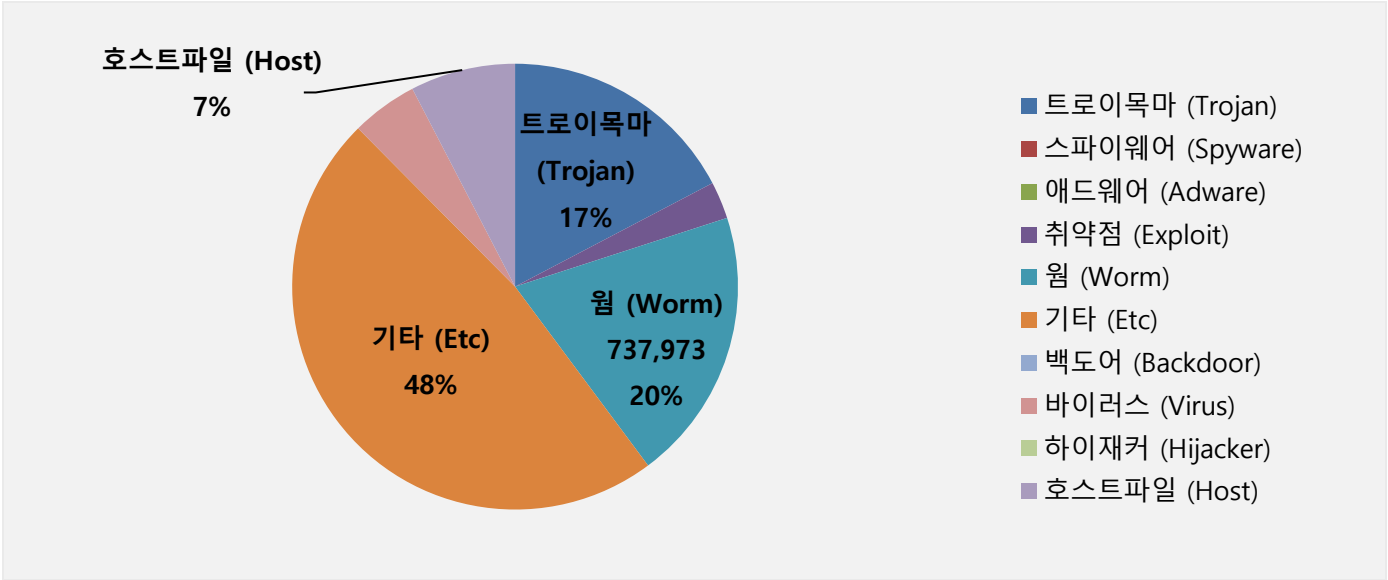
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	New	Worm.ACAD.Bursted	Worm	737,973
2	↑ 1	Gen:Variant.Razy.864420	ETC	494,532
3	↓ 2	Gen:Variant.Razy.767621	ETC	390,280
4	-	Dropped:Trojan.GenericKD.40639357	Trojan	315,372
5	↑ 1	Hosts.media.opencandy.com	Host	283,877
6	↑ 1	Misc.HackTool.AutoKMS	ETC	245,054
7	↓ 2	Gen:Variant.Bulz.624281	ETC	240,431
8	New	Win32.Floxif.Dam	Virus	179,373
9	↑ 5	Gen:Variant.Application.Keygen.16	ETC	169,556
10	New	Gen:Variant.Fugrafa.84058	ERC	131,618
11	↓ 3	Trojan.GenericKD.46767978	Trojan	117,098
12	↓ 10	Trojan.ShadowBrokers.A	Trojan	110,009
13	-	Misc.HackTool.KMSActivator	ETC	106,883
14	↓ 5	Trojan.GenericKDZ.77118	Trojan	102,477
15	-	Exploit.CVE-2010-2568.Gen	Exploit	100,485

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 10 월 01 일 ~ 2021 년 10 월 31 일

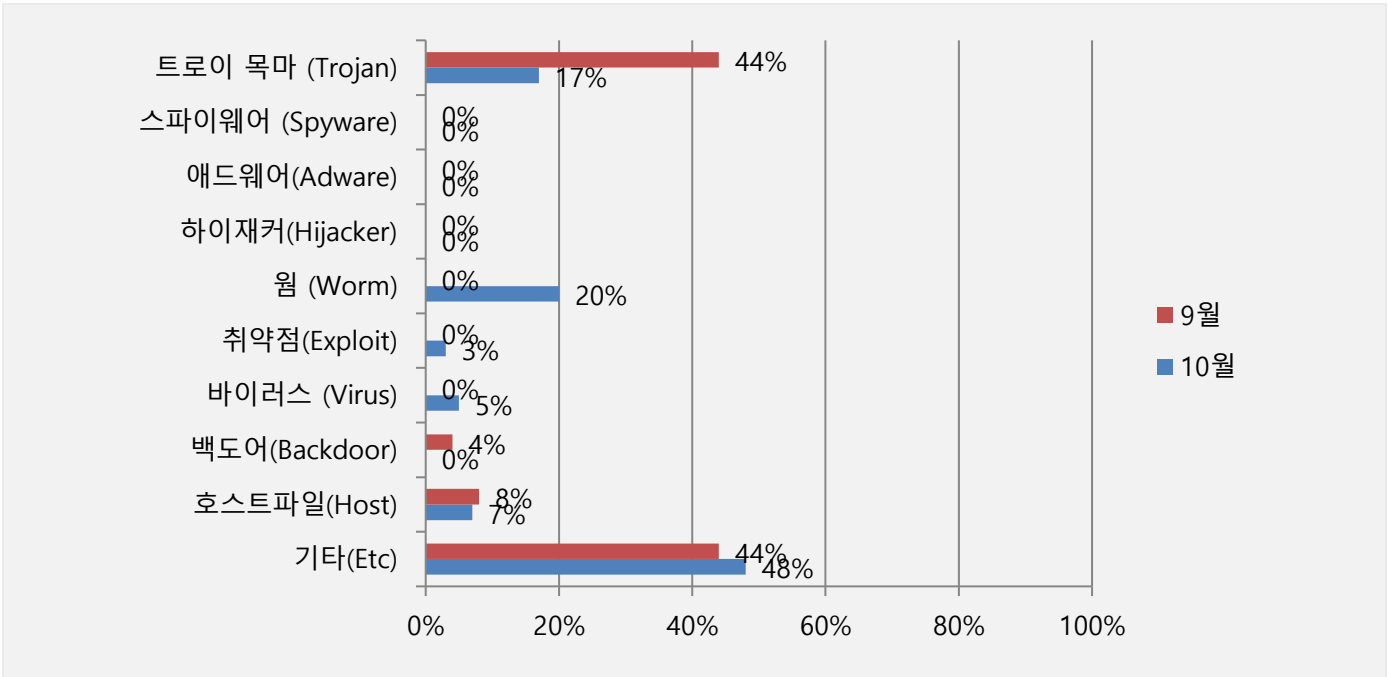
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형과 웜(Worm) 유형이 48%, 20% 비율로 탐지됐으며, 트로이목마(Trojan)와 호스트파일(Host) 유형이 17%와 7%로 그 뒤를 이었다. 2021 년 9 월과 비교하여 전체 감염 건수는 약 35.2% 감소하였다.



카테고리별 악성코드 비율 전월 비교

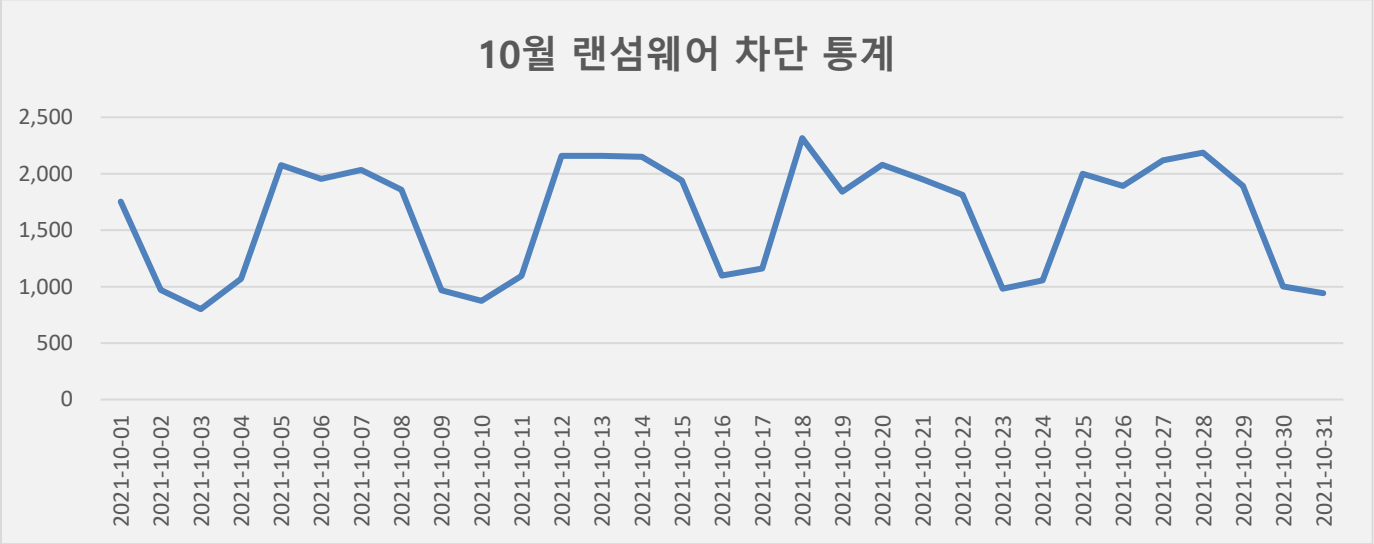
10 월에는 지난 9 월과 비교하여 트로이목마(Trojan) 유형이 61% 감소하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율이 9% 증가했다. 트로이목마는 감소하였지만 웜(Worm)과 바이러스(Virus) 유형이 각 20%, 5%가 증가하여 높은 탐지율을 기록하였다. 지난달에 4%를 기록했던 차지했던 백도어(Backdoor) 악성코드 유형은 이번 달에도 4%를 기록하며 유사한 수치를 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

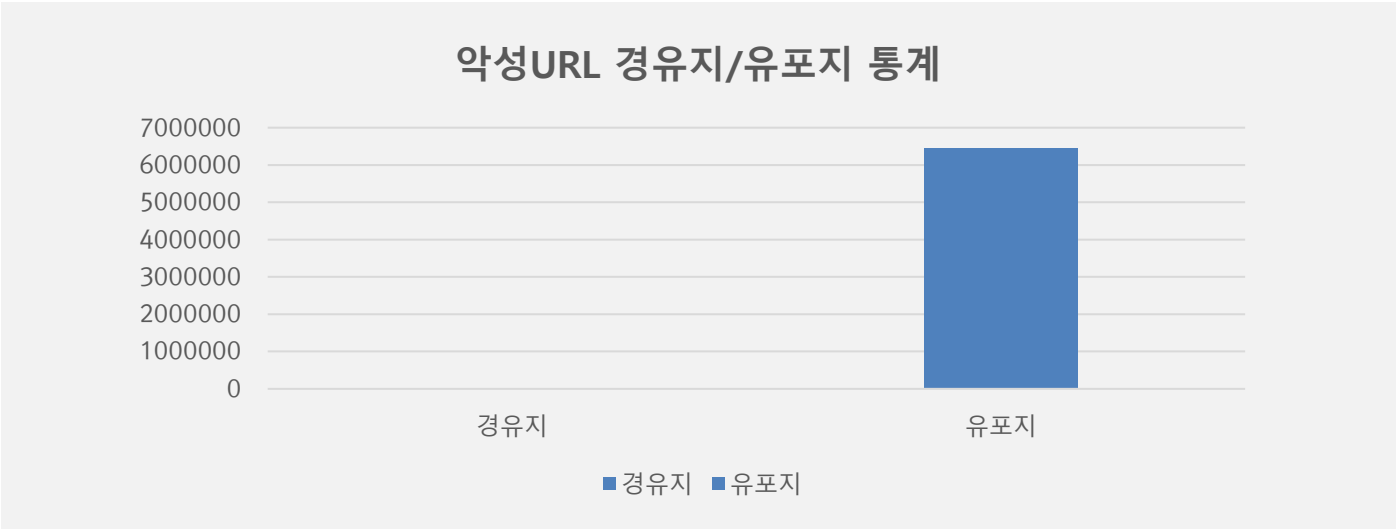
10 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 10 월 1 일부터 10 월 31 일까지 총 50,197 건의 랜섬웨어 공격 시도가 차단되었다. 9 월의 랜섬웨어 공격 건수인 45,706 건에 비해 약 9.8% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한 달간 총 6,472,068 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 9 월 한 달간 확인되었던 6,584,480 의 악성코드 경유지/유포지 URL 수에 비해 약 1.7% 가량 증가한 수치다. 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 바란다.



02
전문가 보안 기고

1. 지속적으로 유포중인 국민비서 사칭 스팸메일 주의!

2. 北 평양과학기술대학 총장을 사칭한 CVE-2021-40444 취약점 공격 주의

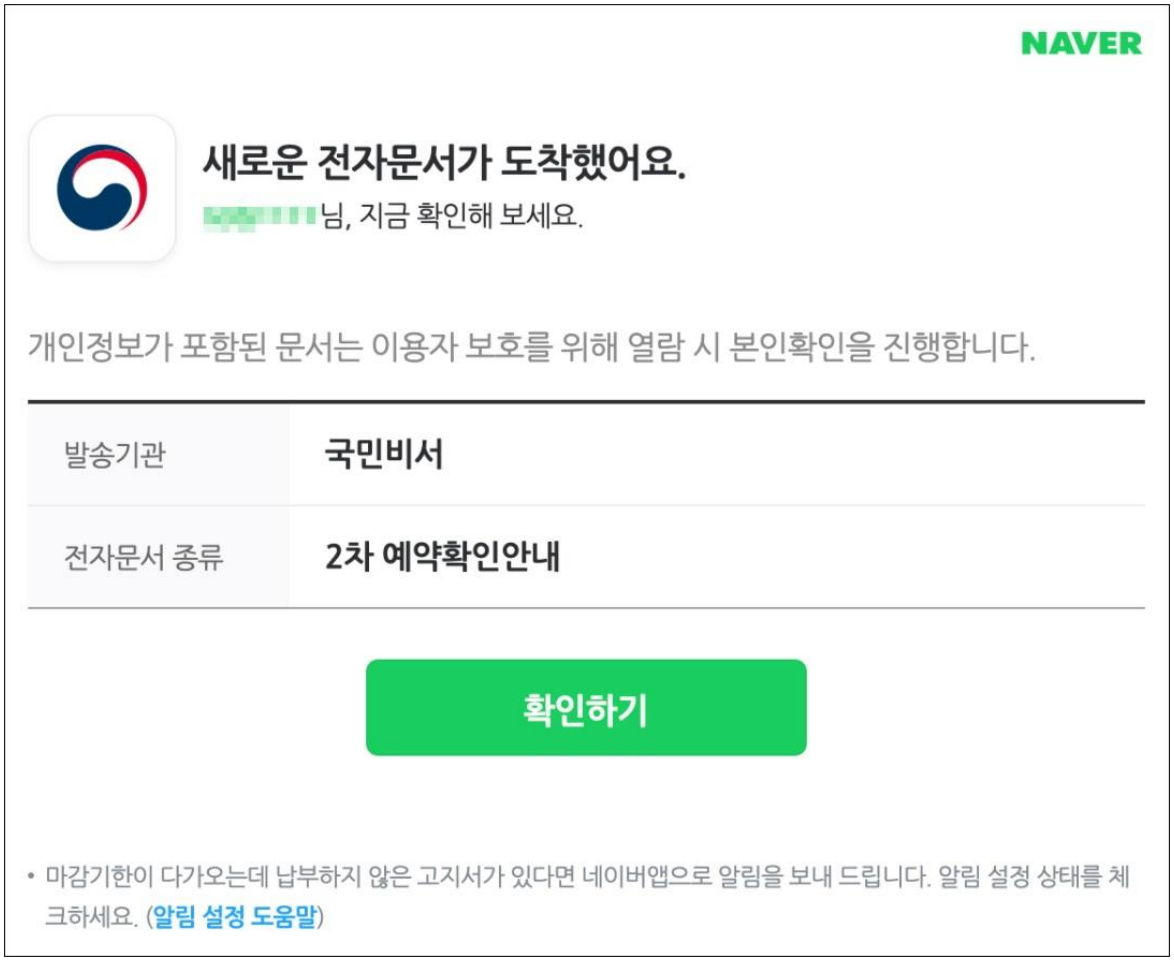
1. 알약 3 분기 랜섬웨어 행위기반 차단 건수: 143,321 건!

최근 국내 백신접종률이 78%를 넘어서고 이미 접종을 마친 국민들을 대상으로 부스터샷도 진행되고 있습니다. 이러한 분위기를 악용하여, 국민비서를 사칭한 피싱 메일이 유포되고 있어 사용자들의 각별한 주의가 필요합니다.

국민비서를 사칭한 피싱 메일에 대해 ESRC 에서는 이미 주의를 권고한 바 있습니다.

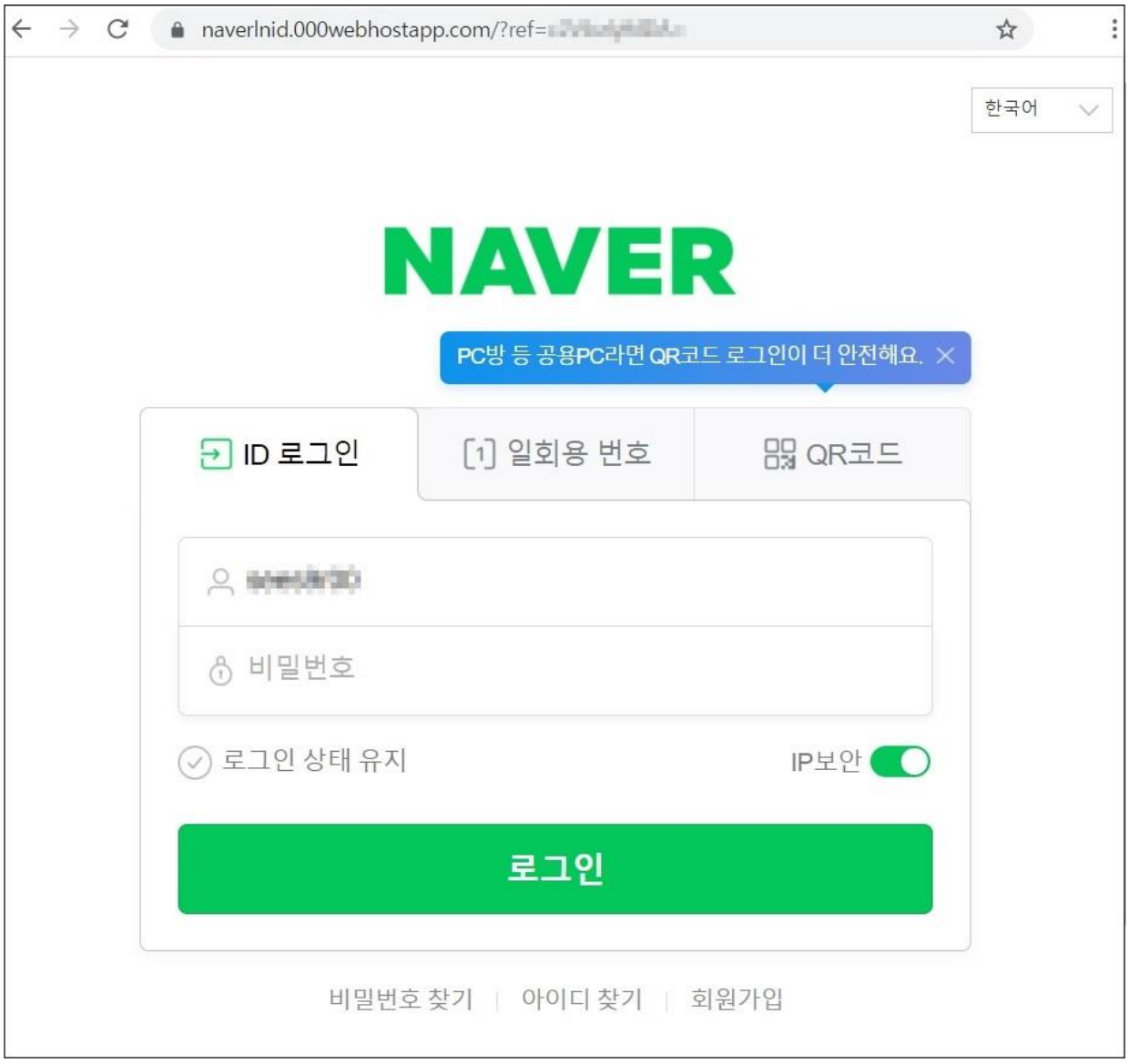
▶ 지속적으로 유포되고 있는 네이버 고객센터 사칭 피싱 메일 주의! (21.10.07)

이번에 발견된 국민비서 사칭 피싱메일 역시 기존에 유포되던 이메일과 동일합니다. 다만, 많은 국민들이 1 차 백신접종이 완료된 점을 고려하여 피싱메일 내용을 2 차예약확인 안내라고 변경하여 유포중입니다.



[그림 1] 국민비서 사칭 피싱메일

확인하기를 누르면, 실제 네이버 로그인 페이지처럼 위장한 피싱 페이지로 이동하며 사용자의 로그인을 유도합니다.



[그림 2] 네이버 로그인 피싱 페이지

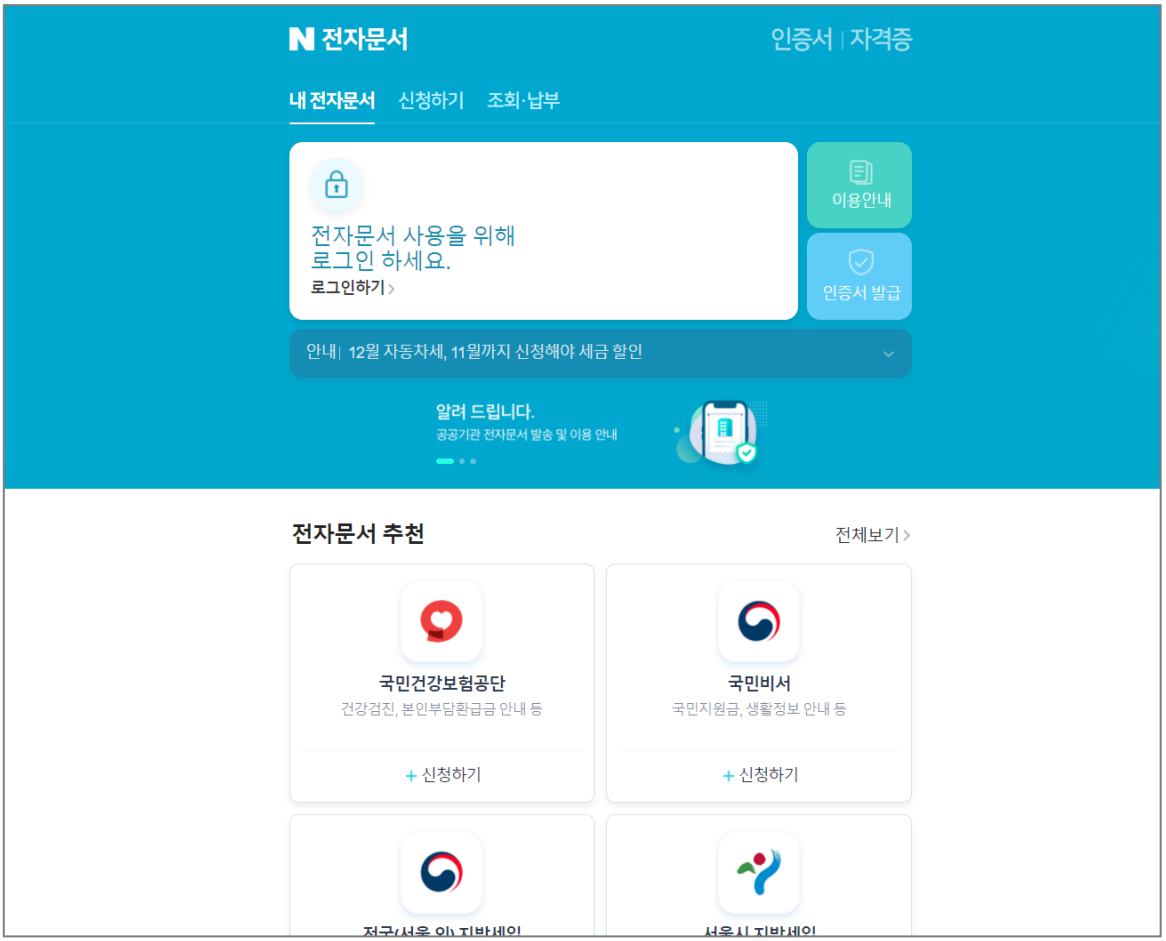
여기에서 사용자는 이미 로그인이 되어있는 상태에서 자신의 메일함에 접속하여 해당 피싱 메일을 열어본 것이기 때문에 또 한번 로그인을 요구하는점을 이상하게 느낄 수 있습니다. 또한 URL 역시 실제 네이버 로그인 주소와 다른 것도 확인할 수 있습니다.

만일 사용자가 로그인을 요구하는 화면만 보고 실제 네이버 로그인 페이지로 오인, 계정정보를 입력한다면 사용자가 비밀번호 오기입 가능성을 배제하고자 비밀번호가 틀렸다며 재입력을 요구하며, 입력한 정보들은 모두 공격자의 서버로 전송됩니다.

Name	Value
id	[redacted]
pwd	[redacted]

[그림 3] 공격자 서버로 전송되는 계정정보

두번째 계정정보 입력 후 로그인 창을 누르면 실제 네이버의 N 전자문서 페이지로 리디렉션 됩니다.



[그림 4] 리디렉션 되는 N 전자문서 페이지

C&C 정보

hxxps://naverlnid.000webhostapp.com/?ref=*******

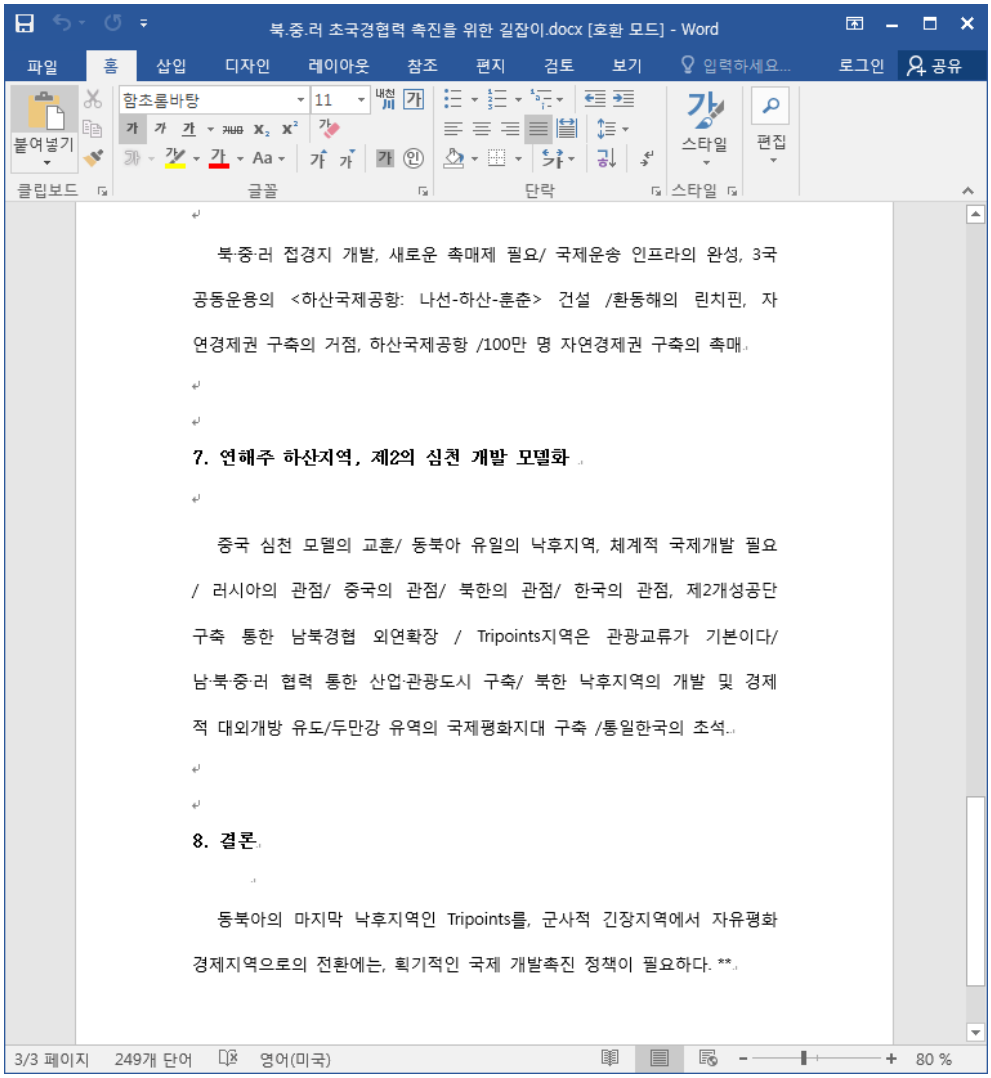
145.14.144.43

네이버를 위장한 피싱 메일이 지속적으로 유포중에 있습니다. 계정정보가 유출 될 경우, 이렇게 유출된 계정정보를 이용한 추가 피해가 예상되는 만큼 사용자들의 각별한 주의가 필요합니다.

사용자 여러분들께서는 접속 페이지의 URL 을 확인하는 습관을 기르시고, 주기적인 비밀번호 변경 및 2 단계 인증을 설정하여 안전한 계정관리를 하시기를 당부 드리겠습니다.

2. 北 평양과학기술대학 총장을 사칭한 CVE-2021-40444 취약점 공격 주의

11 일, 평양 과학기술대학 총장을 사칭한 北 연계 해킹 조직의 공격이 추가로 발견되었습니다. .



[그림 1] CVE-2021-40444 취약점이 포함된 악성 문서 파일

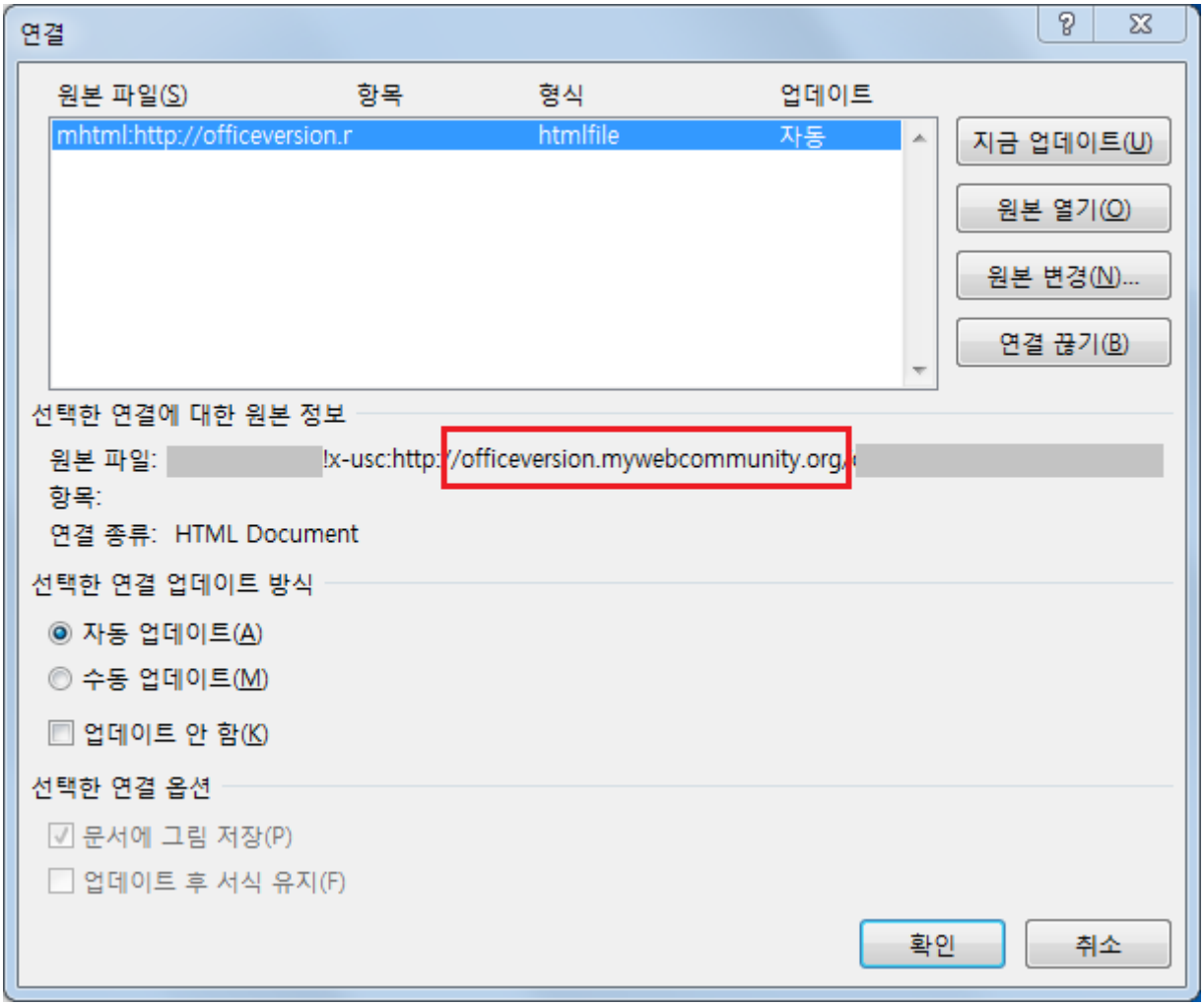
이번 공격은 지난 8 일 보고된 외교·안보·국방·통일분야 전문가를 겨냥한 표적 공격과 마찬가지로 'CVE-2021-40444' 취약점이 동일하게 사용된 것으로 확인되었습니다.

현재 위협 조직이 해당 취약점을 적극적으로 사용하고 있어, MS 오피스 사용자들은 최신 버전으로 즉각 업데이트해야 유사 공격 피해를 사전에 예방할 수 있습니다.

02 전문가 기고

ESRC 에서 이번 공격을 분석한 결과 악성 파일 제작자가 꾸준히 'POSEIDON' 계정을 사용하고 있으며, 이미 인터넷에 공개됐던 'CVE-2021-40444' 취약점의 개념 증명(PoC) 코드를 일부 재활용한 정황을 포착했습니다.

만약 공격 대상자가 MS 오피스 최신 보안 업데이트를 설치하지 않은 상태에서 해당 DOCX 문서를 열어 보안 취약점이 작동되면 'officeversion.mywebcommunity[.]org' 인터넷 주소로 은밀히 통신을 시도하고, 공격자가 지정한 추가 명령에 따라 악성 스크립트가 실행됩니다.



[그림 2] 악성 문서가 연결을 시도하는 인터넷 주소 설정 화면

악성 스크립트가 정상 작동되면, 다음 단계로 'msoffices.atwebpages[.]com' 주소로 연결되고, 후속 명령에 따라 공격자가 개설한 특정 구글 블로그로 접속을 시도하지만, 분석 환경 노출이나 탐지 회피 목적 등으로 일정부분 시차 간격을 두고 연결하는 치밀함도 주목할만한 점입니다. 이후 블로그 게시 글에 포함된 명령에 따라 사용자 컴퓨터 정보를 수집해 공격자 서버로 은밀히 탈취합니다.

02 전문가 기고

ESRC 는 지난 8 일 싱크탱크 행사를 사칭해 국방·안보 분야 전문가를 공격한 내용에 대해 분석하였으며, 이번 사례 역시 'POSEIDON' 계정이 동일하게 사용된 것을 보아 북한 정찰총국 연계 해킹 조직 소행으로 최종 분류 했습니다.

배후로 지목된 북한 사이버 위협 조직이 'CVE-2020-9715', 'CVE-2021-40444' 등 맞춤형 표적 공격에 PDF, DOC 파일과 같은 문서 기반 보안 취약점을 적극 도입하고 있어, 기관 및 기업 보안 관계자들은 최신 업데이트가 유지될 수 있도록 보안 정책 관리가 중요한 시점입니다.

최근 국내에서 최신 보안 취약점을 이용한 APT 공격이 지속적으로 포착되고 있어 사용중인 운영체제와 응용프로그램은 항상 최신 버전으로 유지하는 노력이 필요합니다. 또한 대북 분야 종사자들은 특히 북한의 사이버 공격을 받을 수 있다는 경각심을 가져야 하겠습니다.

이번 악성파일에 대해 현재 알약에서는 Exploit.CVE-2021-40444 로 탐지중에 있으며, 피해 확산 방지를 위한 대응 조치를 한국인터넷진흥원(KISA) 등 관련 부처와 긴밀하게 협력하고 있습니다.

03
악성코드 분석 보고

[Spyware.CryptBot] 악성코드 분석 보고서

최근 'Spyware.CryptBot'(이하 'CryptBot') 정보 탈취 악성코드가 가짜 소프트웨어 사이트 등을 통해 유포되고 있는 것으로 알려져 있다. 이 악성코드에 감염이 되는 경우, 정보 탈취 및 클립보드를 공격자 지갑 주소로 변경하는 추가 페이로드 다운로드 기능을 수행하게 되어 금전적으로 상당한 피해가 발생할 수 있다.

```
GdiplusStartup(&v41, &Rect.top, 0);
v10 = GetDesktopWindow();
GetWindowRect(v10, &bmi.bmiHeader.biClrUsed);
v11 = GetWindowDC(v10);
v45 = (*bmi.bmiColors - bmi.bmiHeader.biClrUsed);
h = v11;
v44 = Rect.left - bmi.bmiHeader.biClrImportant;
LOWORD(v10) = GetDeviceCaps(v11, 12);
v12 = CreateCompatibleDC(v11);
v32 = v45;
LOWORD(bmi.bmiHeader.biSize) = 1;
v31 = 40;
ppvBits = -v44;
HIWORD(bmi.bmiHeader.biSize) = v10;
bmi.bmiHeader.biWidth = 0;
bmi.bmiHeader.biHeight = 0;
*&bmi.bmiHeader.biPlanes = 0;
bmi.bmiHeader.biCompression = 0;
bmi.bmiHeader.biSizeImage = 0;
bmi.bmiHeader.biXPelsPerMeter = 0;
bmi.bmiHeader.biYPelsPerMeter = 0;
v43 = CreateDIBSection(h, &v31, 1u, &v30, 0, 0);
if ( !v43 )
{
  DeleteDC(v12);
  DeleteDC(h);
  GdiplusShutdown(v41);
}
v13 = SaveDC(v12);
SelectObject(v12, v43);
BitBlt(v12, 0, 0, v45, v44, h, 0, 0, 0xCC0020u);
```

[그림] 스크린샷 수집 코드 일부

'CryptBot'는 감염 PC 정보, 웹 브라우저 크리덴셜, 암호화폐 애플리케이션 정보를 탈취하여 C&C 전송, 추가 페이로드 다운로드 기능을 수행한다. 그리고 다운로드되어 실행되는 'ClipBanker'는 사용자의 클립보드에 암호화폐 지갑 문자열이 존재하는 경우, 이를 공격자 지갑으로 변조하는 기능을 가진다.

다른 정보 유출형 악성코드와 달리 암호화폐 탈취에 많은 부분이 집중되어 있어서, 암호화폐를 자주 이용하는 기업, 개인 입장에서 이 악성코드에 감염이 된다면 상당한 금전적인 피해가 발생될 수 있다.

따라서 악성코드 감염을 예방하기 위해 출처가 불분명한 웹 사이트에서의 다운로드를 지양해야 하며, 신뢰할 수 있는 백신을 항상 최신 버전으로 유지해야 한다.

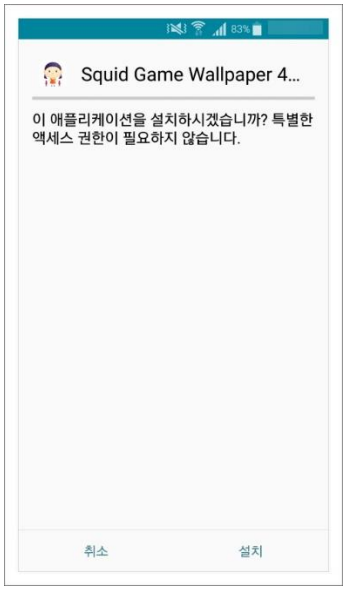
현재 알약에서는 해당 악성코드들에 대해 'Spyware.CryptBot', 'Trojan.Clipbanker.A'로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Agent] 악성코드 분석 보고서

최근 한국의 콘텐츠인 '오징어게임'이 전 세계적인 흥행에 성공하고 있다. 그리고 이런 기회를 적극적으로 이용하려는 공격자들은 '오징어게임'과 연관되어 있는 듯한 악성 앱들을 발빠르게 제작하여 유포하고 있다.

지난 10 월 발견된 이 악성 앱은 '오징어게임' 월 페이퍼 앱으로 위장하여 유포되었다.

이 악성 앱을 설치하면 추가적인 라이브러리와 플러그인 패키지를 다운받아 피해자가 원하지 않는 광고를 구독하게 된다. 물론 피해자는 광고 관련 페이지를 볼 수 없도록 제작되었기에 실제 피해를 체감하지는 못한다.



[그림] 악성 앱 설치 화면

이런 악성 앱들은 피해자들의 데이터와 스마트폰 자원을 활용하여 수익 실현을 하지만 피해자들은 구체적인 피해 상황이 드러나지 않기에 이를 쉽사리 인지하기 어렵다.

따라서, 출처가 불명확한 URL 과 파일은 실행하지 않아야 하며 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫 걸음이라 할 수 있을 것이다.

현재 알약 M 에서는 해당 앱을 'Troan.Android.Agent' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

Telegraph, 가입자 정보 포함 10TB 데이터베이스 노출시켜

The Telegraph exposes 10 TB database with subscriber info

영국 최대 신문사이자 온라인 매체 중 하나인 Telegraph 의 데이터베이스 중 하나가 제대로 보호되지 않아 데이터 10TB 가 유출되는 사고가 발생했습니다.

노출된 정보에는 내부 로그, 전체 가입자 이름, 이메일 주소, 기기 정보, URL 요청, IP 주소, 인증 토큰, 고유한 독자 식별자가 포함됩니다.

보안 연구원인 Bob Diachenko 는 지난 9 월 14 일 보호되지 않은 데이터 셋을 발견했으며 당시 암호화되지 않은 연락처에 최소 1,200 건에 비밀번호 없이도 접근이 가능함을 확인했습니다.

[그림] 노출된 기록 샘플

[이미지 출처] https://cooltechzone.com/leaks/the-telegraph-giant-data-leak

특히, 이들 중 다수는 Apple News 구독자 정보에도 영향을 미치며 비밀번호를 평문 상태로 포함하고 있었습니다. 해당 신문사는 노출 사고에 대해 즉시 제보를 받았지만, 결국 대응 및 데이터베이스 보호에 이틀이 소요되었습니다.

해당 인스턴스는 2021 년 9 월 1 일에 전문 검색 엔진에 인덱싱되었기 때문에 예상되는 노출 기간은 최소 3 주입니다. 공격자와 자동화된 스캐너가 노출된 데이터베이스를 찾아 저장된 데이터를 추출하기에 충분한 시간입니다.

일부 구독자만 영향 받아 이 사고로 데이터가 유출된 피해자가 겪을 수 있는 가장 큰 위험은 이메일을 통한 사기나 피싱을 당하는 것입니다.

URL 요청이 유출될 경우 누군가가 이를 통해 뉴스 플랫폼에서 사용자의 검색 기록을 알아낼 수 있기 때문에 개인정보 보호 관련 위험이 발생할 수도 있습니다.

Telegraph 의 경우 비구독자가 훔친 액세스 토큰을 통해 유료 콘텐츠에 접근할 수 있지만, 이는 리셋을 통해 해결할 수 있습니다.

Telegraph 는 Diachenko 의 제보와 관련해 아래와 같이 입장을 발표했습니다.

"지난 9월 16일에 이 사고에 대해 알게 되었으며 데이터를 보호하기 위한 즉각적인 조치를 취했습니다. 조사에 따르면 기록 중 소수만 노출된 것으로 나타났습니다. 전체 사용자의 0.1% 미만이며, 모든 사용자에게 연락을 취해 해당 사실을 알렸습니다. 또한 조사 결과 데이터가 노출된 상태였던 동안 해당 연구원이 공개한 데이터 이외에는 침해되지 않았다는 결론을 내렸습니다. 취약점과 노출을 책임감 있게 공개한 연구원의 작업에 매우 감사드립니다."

회사의 입장문에 따르면, 영향을 받은 사용자의 수는 600 명으로 Daichenko 가 언급한 수 보다 적습니다. 또한 Telegraph 는 Diachenko 가 민감 데이터 셋에 접근한 최초이자 마지막 사람이기 때문에 다른 사람이 접근했을 위험은 없을 것이라 밝혔습니다.

Telegraph 에 가입했을 경우 비밀번호를 재설정하고, 예상하지 않은 이메일에 주의하여 계정을 보호하는 것이 좋습니다.

[출처]

https://www.bleepingcomputer.com/news/security/the-telegraph-exposes-10-tb-database-with-subscriber-info/

https://cooltechzone.com/leaks/the-telegraph-giant-data-leak

화웨이 클라우드 노리는 업데이트된 크립토마이너 발견

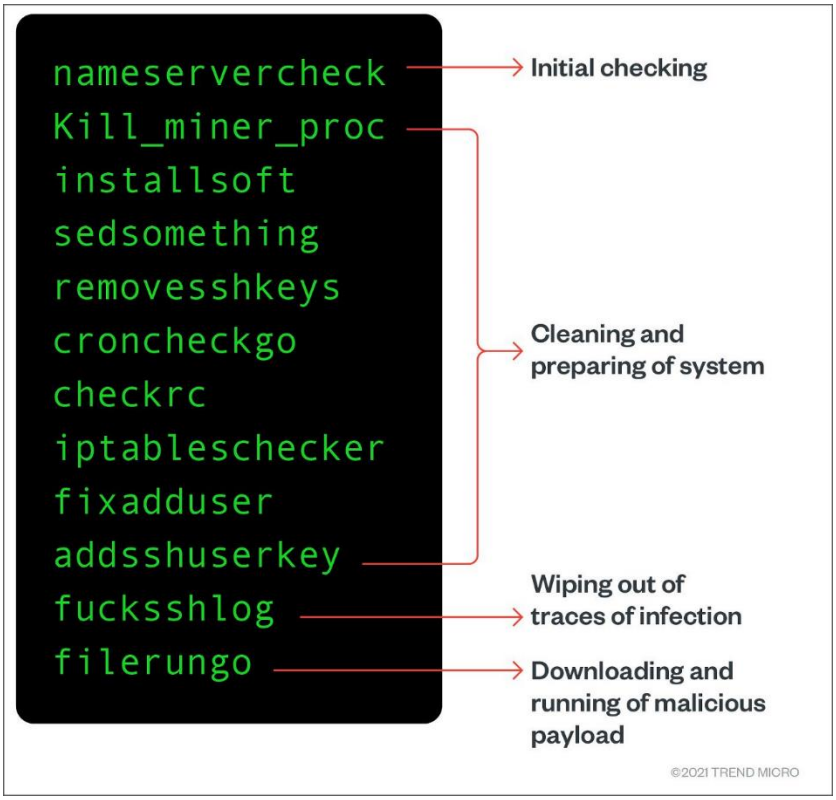
Huawei Cloud targeted by updated cryptomining malware

지난 2020 년 Docker 컨테이너를 공격하는 데 사용된 리눅스용 크립토마이너의 새 버전이 이제 화웨이 클라우드를 비롯한 클라우드 서비스 제공업체를 노리기 시작한 것으로 보입니다.

Trend Micro 의 연구원은 이 새로운 캠페인을 분석하여 해당 악성코드가 이전 기능을 유지하면서 새로운 기능을 추가해 어떻게 진화했는지 설명했습니다.

최신 샘플은 방화벽 규칙 생성 기능을 주석 처리했으며, API 관련 포트로 다른 호스트를 매핑하기 위한 네트워크 스캐너를 계속 드롭합니다. 새로운 악성코드 버전은 클라우드 환경만을 노리며, 이전에 시스템을 감염시킨 다른 크립토재킹 스크립트를 찾아 제거합니다.

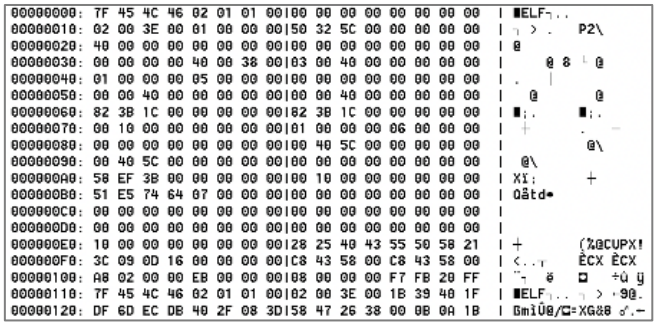
이 악성 크립토마이너는 리눅스 시스템을 감염시킬 때 다른 크립토마이닝 악성코드 배포자가 생성한 사용자를 제거하는 작업을 수행합니다.



[그림] 바이너리 배포 다이어그램

[이미지 출처] https://www.trendmicro.com/en_us/research/21/j/actors-target-huawei-cloud-using-upgraded-linux-malware-.html

드롭된 바이너리("linux64_shell", "ff.sh", "fczyo", "xlinux")는 어느 정도 난독화가 되어있으며, 연구원들은 래핑을 위해 UPX 패커가 배포된 징후를 발견했습니다.



[그림] 바이너리에서 발견한 UPX 헤더

[이미지 출처] https://www.trendmicro.com/en_us/research/21/j/actors-target-huawei-cloud-using-upgraded-linux-malware-.html

공격자들은 자동화된 분석 및 탐지 툴을 통해 발견되지 않기 위해 바이너리를 조정할 목적으로 추가적인 변조 단계를 거쳤습니다. 기기에 침투할 발판을 마련한 후, 해커의 스크립트는 원격으로 시스템을 악용하고 악성 스크립트와 크립토마이너에 감염시킵니다.

이 공격에서 검색한 알려진 취약점은 아래와 같습니다.

- 취약한 SSH
- Oracle Fusion Middleware 의 Oracle WebLogic Server 제품 내 취약점(CVE-2020-14882)
- Redis 무단 액세스 또는 취약한 자격 증명
- PostgreSQL 무단 액세스 또는 취약한 자격 증명
- 취약한 SQLServer 자격 증명
- MongoDB 무단 액세스 또는 취약한 자격 증명
- 취약한 FTP 자격 증명

화웨이 클라우드는 비교적 새로운 서비스이지만, 이미 300 만 명이 넘는 고객에게 서비스를 제공하고 있다고 주장했습니다. Trend Micro 는 화웨이 측에 이 캠페인에 대해 알렸지만 아직까지 답변을 받지 못했습니다.

취약점 평가 또는 악성코드 검사를 실행하는 것만으로는 이 공격을 충분히 방어해낼 수 없습니다. CSP 의 보안 모델을 평가하고 접근 방식을 조정하여 추가 보호 기능으로 보완해야 합니다.

이러한 클라우드를 노리는 크립토마이너는 연초부터 증가하고 있으며, 가상화폐의 가치가 치솟는 한 공격자들은 더욱 강력해지고 탐지를 어렵게 만들 방법을 찾을 것입니다.

[출처]

https://www.bleepingcomputer.com/news/security/huawei-cloud-targeted-by-updated-cryptomining-malware/

https://www.trendmicro.com/en_us/research/21/j/actors-target-huawei-cloud-using-upgraded-linux-malware-.html

백만 안드로이드 사용자, 구독 사기 캠페인의 타깃이 돼

Millions of Android users targeted in subscription fraud campaign

대규모 사기 캠페인에서 총 1,050 만회 다운로드된 안드로이드 앱 151 개를 사용해 사용자가 자신도 모르는 사이 유료 구독 서비스에 가입하도록 속인 것으로 나타났습니다. 해당 캠페인을 발견한 Avast 의 연구원은 이를 'UltimaSMS'라 명명했으며, 구글 플레이 스토어에서 관련 앱 80 개를 찾아 제보했습니다.

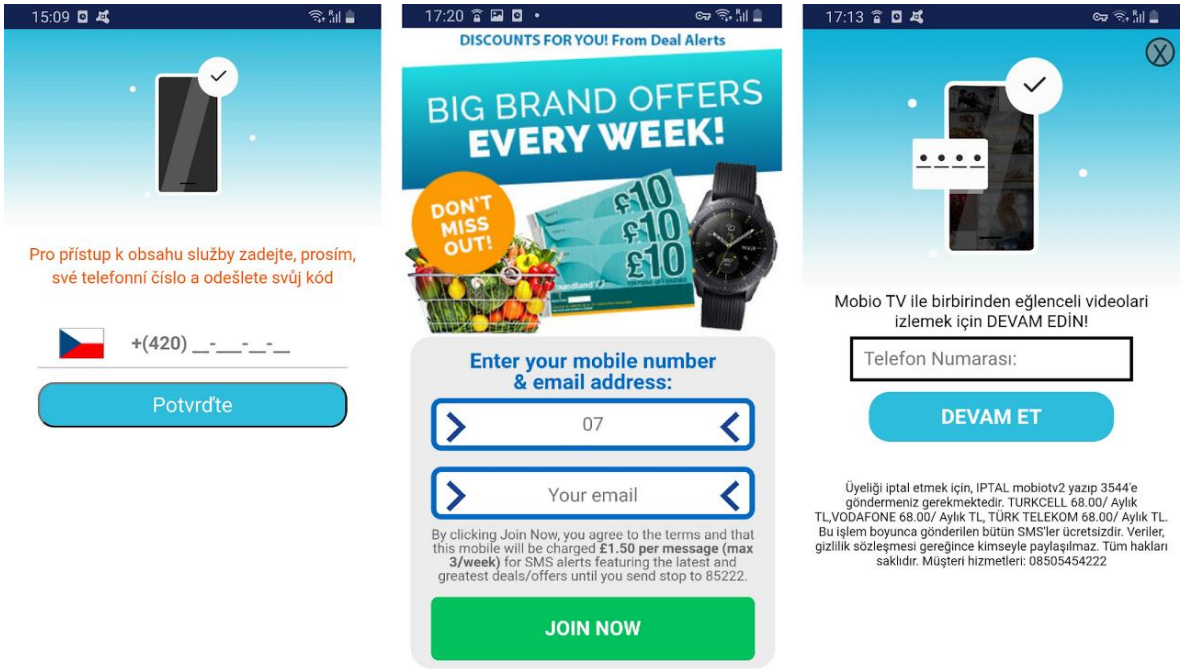
구글은 앱을 빠르게 제거했지만, 사기꾼은 그 동안 구독 요금으로 이미 수백만 달러를 벌어들였을 가능성이 큰 것으로 나타났습니다.

공격은 전화번호로 시작돼

공격자는 할인 앱, 게임, 맞춤형 키보드, QR 코드 스캐너, 영상/사진 편집기, 스팸 전화 차단기, 카메라 필터 등으로 위장한 안드로이드 앱 151 개를 통해 UltimateSMS 캠페인을 수행했습니다.

위의 앱은 처음 실행되면 위치, IMEI 등 스마트폰의 데이터를 확인 후 국가에 맞게 언어를 변경합니다.

이후 해당 앱은 사용자에게 프로그램 기능에 액세스하기 위해서 휴대폰 번호와 이메일 주소를 입력하라는 메시지를 표시합니다



[그림] 사기 앱 중 일부의 첫 화면

[이미지 출처] https://blog.avast.com/premium-sms-scam-apps-on-play-store-avast

이 앱은 전화번호와 필요한 권한을 얻어낸 후 피해자를 월 40 달러 SMS 서비스에 가입시킵니다. 사기꾼은 해당 서비스의 제휴 파트너로 분배금을 받습니다.

Avast 의 분석에 따르면, 이러한 앱의 제작자는 피해자의 위치에 따라 청구가 가능한 최대 금액을 청구하는 시스템을 구현했습니다.

이러한 앱의 대부분은 홍보에 이용된 기능을 제공하지 않고, 플레이 스토어에도 수 많은 부정적인 리뷰가 등록되어 있는 상태입니다. 하지만 제작자는 여전히 엄청난 양의 앱을 등록해 공격에 지속적으로 성공하고 있습니다. UltimaSMS 캠페인에 이렇게 많은 앱을 사용하여 사기꾼은 지속적인 신고 및 구글의 게시 중단 조치에도 불구하고 지속적으로 피해자를 양산하고 플레이 스토어에 남아있을 수 있었습니다.

Sensor Tower 에 따르면 가장 많은 피해를 입은 국가는 이집트, 사우디아라비아, 파키스탄, UAE 이며 피해자는 모두 100 만 명이 넘었습니다. 미국에서는 기기 17 만대가 감염된 것으로 나타났습니다.

Country	Downloads
Egypt	2,600,000
Saudi Arabia	2,400,000
Pakistan	2,000,000
United Arab Emirates	1,000,000
Turkey	790,000
Oman	400,000
Qatar	450,000
Kuwait	200,000
US	170,000
Poland	170,000

[그림] 캠페인의 영향을 가장 많이 받은 국가
[이미지 출처] https://www.bleepingcomputer.com/news/security/millions-of-android-users-targeted-in-subscription-fraud-campaign/

UltimateSMS 피해자가 해야할 일

앱을 제거하면 새로운 구독이 발생하는 것을 막을 수는 있지만, 이전에 구독한 서비스가 재구독되는 것을 막지는 못합니다. 이후 요금이 부과되지 않도록 하려면 통신사에 연락해 모든 SMS 서비스의 구독 취소 요청을 해야합니다.

기기에서 즉시 제거해야 하는 앱의 전체 목록은 여기에서 확인하실 수 있습니다.

이러한 사기에 피해를 입지 않으려면 이동통신사에 연락하여 계정에 대한 유료 SMS 옵션을 비활성화하고, 필수가 아닌 경우 앱에 전화번호를 입력하지 않아야 합니다.

또한 앱을 설치하기 전에 리뷰를 읽고 부정적인 피드백이 많을 경우 앱을 설치하지 말아야 합니다.

[출처]

https://www.bleepingcomputer.com/news/security/millions-of-android-users-targeted-in-subscription-fraud-campaign/

https://blog.avast.com/premium-sms-scam-apps-on-play-store-avast

https://github.com/avast/ioc/blob/master/UltimaSMS/UltimaSMS_IOC_19-10-2021.pdf

(주)이스트시큐리티

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