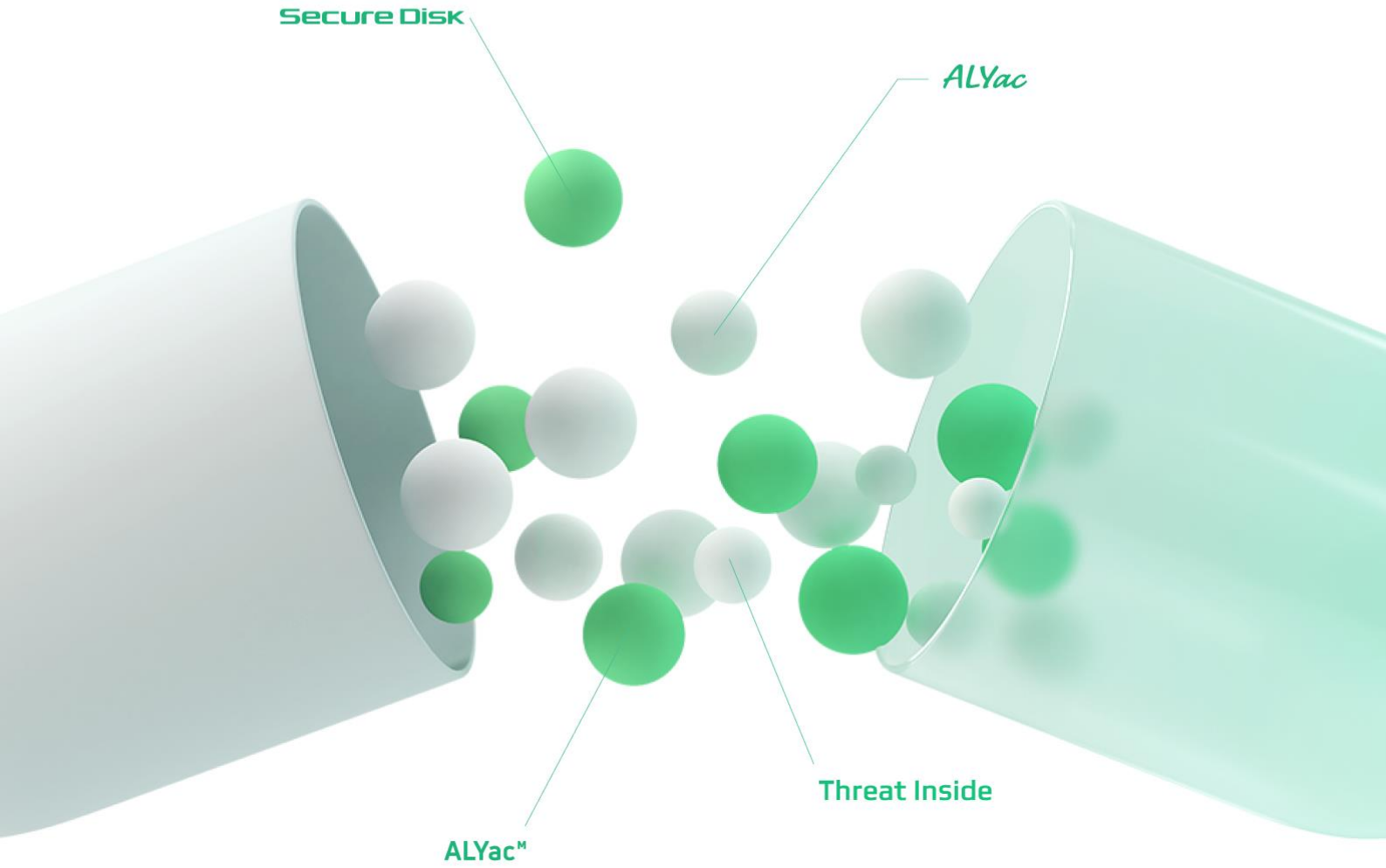
이스트시큐리티
보안동향보고서

No.153
2022/06/27

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외보안동향을 확인하세요.



이스트시큐리티 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

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

1. 악성코드 동향

2022년 5월에는 악명 높은 사이버 범죄 갱단인 레빌(Revil)이 다시 운영을 시작했으며, 리눅스와 윈도우시스템을 노리는 새로운 봇넷 Sysr-K가 등장했습니다. 이외에도 Fillina 제로데이, Clolp랜섬웨어, 이모텟(Emotet), 금성121, 비너스락커, 페이커스트라이커 조직으로 추정되는 APT 공격까지 다양한 보안 위협이 발견되었습니다.

레빌(Revil) 랜섬웨어는 지난 10월 국제적 공조로 인해 공격용 토르 서버가 폐쇄되었는데 최근 러시아와 우크라이나 침공 이후 다시 활동을 시작했습니다. 새로운 레빌 랜섬웨어 샘플에는 기존 소스코드에서 “accs” 필드가 추가되었으며 이는 특정 피해자의 크리덴션이 포함되어 고도의 타킷화 된 공격을 하기 위한 준비로 추측되고 있습니다.

리눅스와 윈도우시스템을 노리는 Sysrv의 변종 Sysrv-K 악성코드는 기존 봇넷의 역할을 수행하면서 감염 된 타겟에서 암호화폐 채굴까지 진행됩니다. 또한 이번 변종에서는 WordPress의 구성 파일과 백업을 검색해 데이터베이스 크리덴션을 가져와 웹 서버를 획득할 수 있습니다.

Follina 제로데이 취약점은 5월에 나온 취약점으로 매크로가 비활성화 된 경우에도 MSDT를 통해 코드를 실행할 수있으며 이는 취약점이 확인 된 Word 문서에서 External 태그에 작성 된 URL을 통해 악의적인 코드 실행이 가능합니다.

이외에도 북한이탈주민 자문위원대상 의견수렴 설문지 문서, 한국정책방송원의 유튜브 방송 출연 섭외로 위한한 HWP 악성문서, 국내 주요 관공서 이력서와 저작권과 관련 된 이메일 공격 등 이메일을 통한 APT 공격이 지속적으로 발견되고 있기 때문에 사용자는 출처를 알 수 없는 메일에 첨부된 파일 및 URL을 절대 클릭하기 않아야 하며 정부 기관 및 잘 알려진 조직으로부터 전달된 메일이라도 항상 의심하고 주의하는 보안 의식이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2022년 5월의 감염 악성코드 Top 15 리스트에서는 국내 광고 소프트웨어를 설치하는 Hosts.media.opencandy.com 악성코드가 541,661건에서 1,433,546건으로 약 164% 크게 증가하여 국내 광고 소프트웨어가 지속적으로 발견되고 있으며, 지난달에 이어 오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted, Trojan.Lisp.Agent.f 도 증가율을 보여주고 있다.

Lnk 취약점인 CVE-2010-2568를 사용하는 악성코드가 새롭게 Top 15에 등장할 만큼 5월에는 관련된 악성코드가 많이 발견되었다.

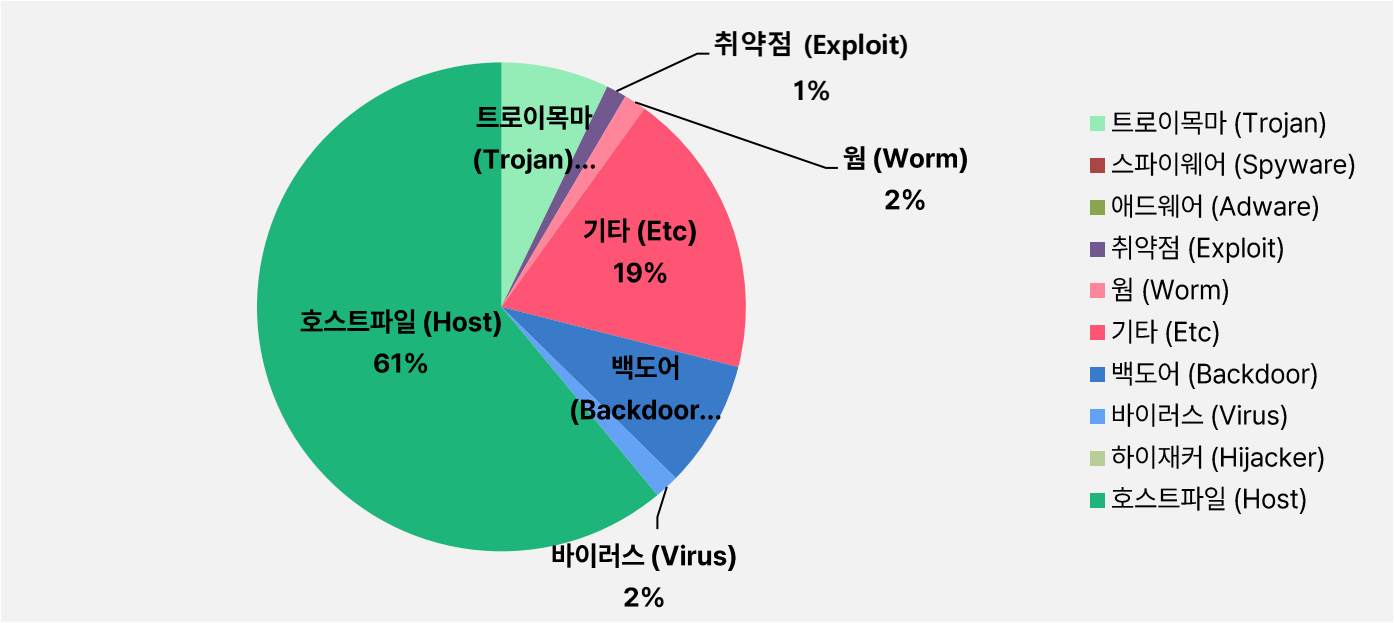
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	1,433,546
2	-	Backdoor.Generic.792814	Backdoor	197,314
3	New	Gen:Variant.Razy.360325	ETC	167,230
4	↓1	Misc.HackTool.AutoKMS	ETC	79,196
5	↑3	Trojan.Lisp.Agent.F	Trojan	77,659
6	-	Trojan.Damaged.PE	Trojan	59,964
7	-	Misc.HackTool.KMSActivator	ETC	51,846
8	↑6	Gen:Variant.Razy.864420	ETC	44,747
9	↓4	Win32.Neshta.A	Virus	38,282
10	-	Application.Hacktool.KMSActivator.AI	ETC	36,186
11	New	Gen:Variant.Fugrafa.3766	ETC	35,275
12	New	Worm.ACAD.Bursted	Worm	34,606
13	-	Application.Hacktool.KMSActivator.HA	ETC	32,241
14	New	Exploit.CVE-2010-2568.Gen	Exploit	31,537
15	↓6	JS:Trojan.Cryxos.5175	Trojan	29,877

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022년 5월 01일 ~ 2022년 5월 31일

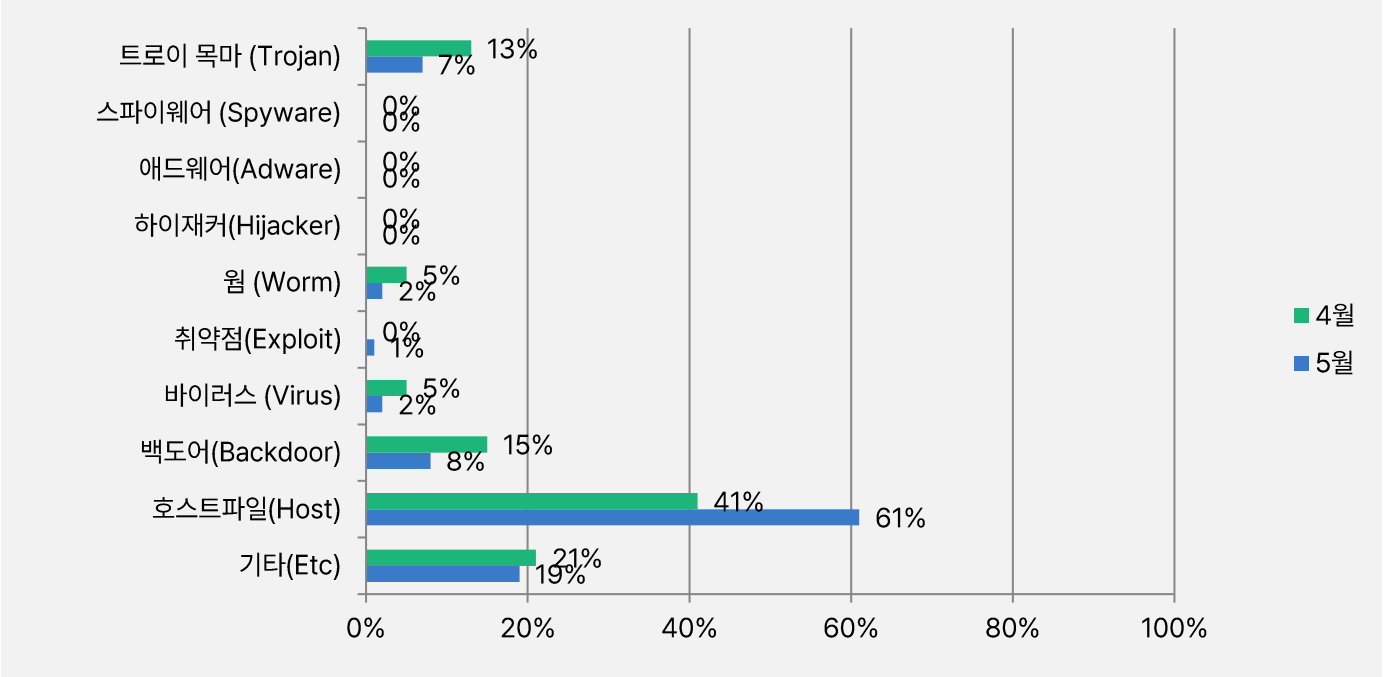
악성코드 유형별 비율

악성코드 유형별 비율에서 호스트파일(Host) 이 지난달에 이어 41%로 가장 높은 비율로 탐지 되었으며, 기타(ETC) 유형과 백도어(Backdoor) 유형이 21%, 15%로 트로이목마(Trojan)와 웜(Worm) 유형이 13%, 5%로 확인되었다. 바이러스(Virus) 유형이 새롭게 5%로 확인되었다. 2022년 3월과 비교하여 전체 감염 건수는 약 11.9% 감소하였다.



카테고리별 악성코드 비율 전월 비교

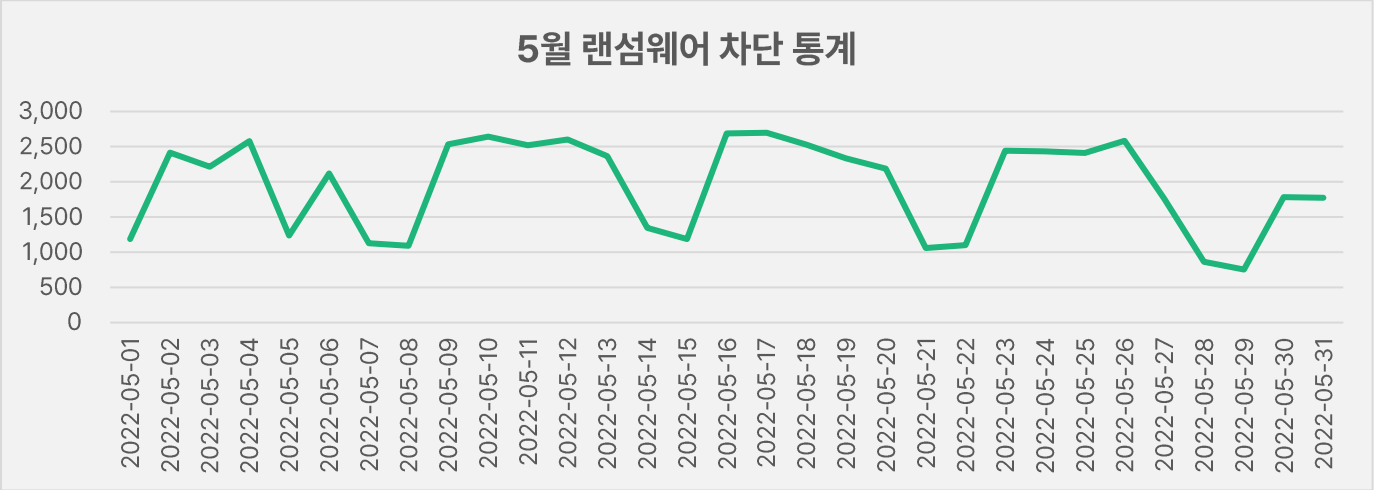
2022년 5월에는 지난 4월과 비교하여 호스트파일(Host) 유형의 악성코드 감염이 20% 크게 증가하면서 지속적인 높은 탐지율을 기록하고 있으며, 호스트파일(Host) 유형을 제외한 기타(ETC), 백도어(Backdoor), 트로이목마(Trojan), 웜(Worm), 바이러스(Virus)는 전체적으로 3~7% 감소하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

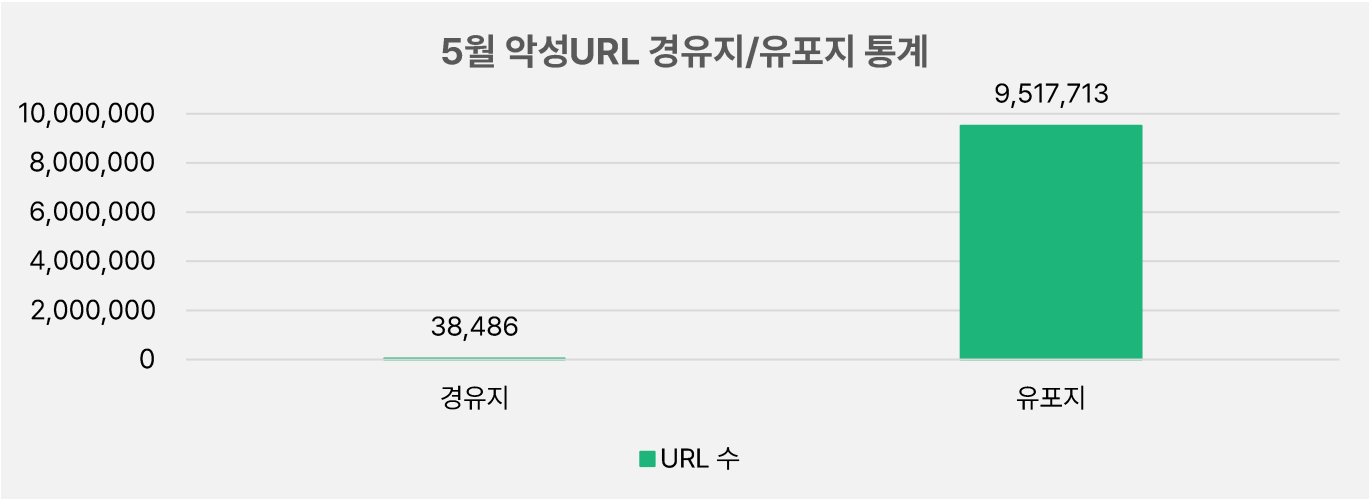
5월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 5월 1일부터 5월 31일까지 총 60,561건의 랜섬웨어 공격 시도가 차단되었다. 4월의 랜섬웨어 공격 건수인 61,582건에 비해 약 1.6% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 5월 한 달간 총 9,556,199건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 4월 한 달간 확인되었던 7,291,876의 악성코드 경유지/유포지 URL 수에 비해 약 31% 가량 증가한 수치다. 악성코드 경유지/유포지 URL의 경우 항상 고정적인 URL만 모니터링하는 것이 아닌, 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바란다.



2

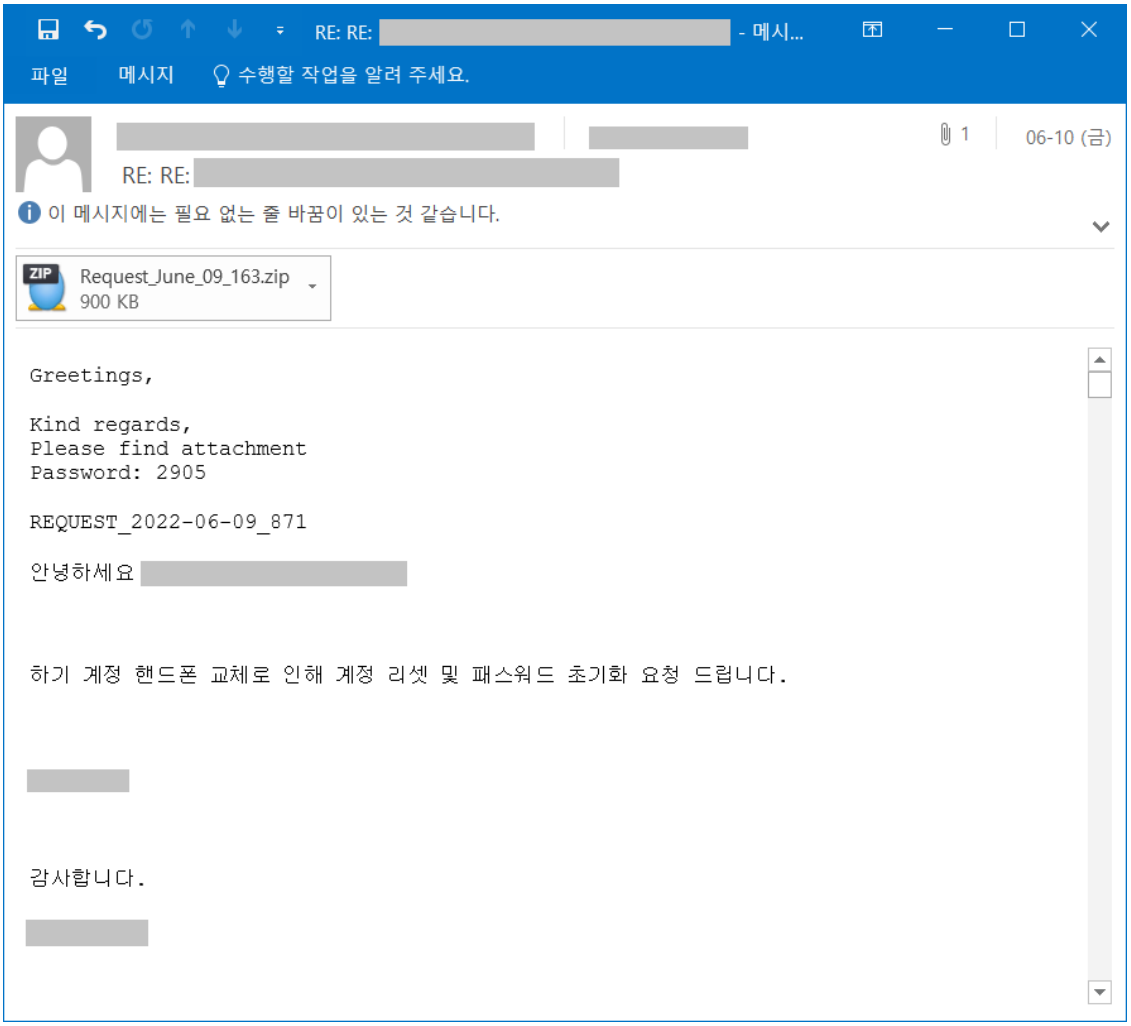
전문가 보안 기고

1. ISO 첨부파일을 통해 유포되고 있는 범블비(Bumblebee) 악성코드 주의!

2. 북한이탈주민(탈북민) 자문위원대상 의견수렴 설문지 위장 **北** 연계 해킹 주의!

1. ISO 첨부파일을 통해 유포되고 있는 범블비(Bumblebee) 악성코드 주의!

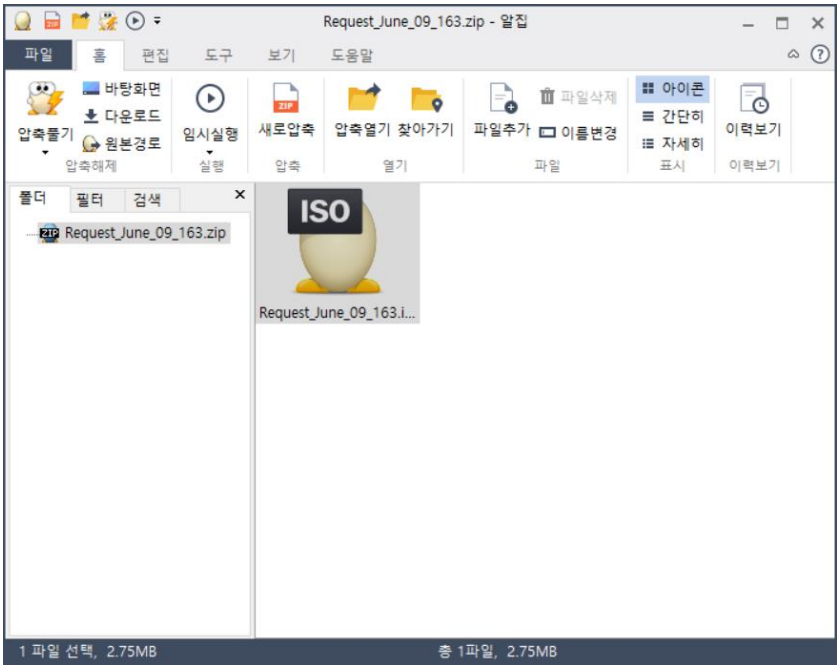
ISO 첨부파일을 통해 범블비(Bumblebee) 악성코드가 국내에 유포 중에 있어 사용자들의 주의가 필요합니다.



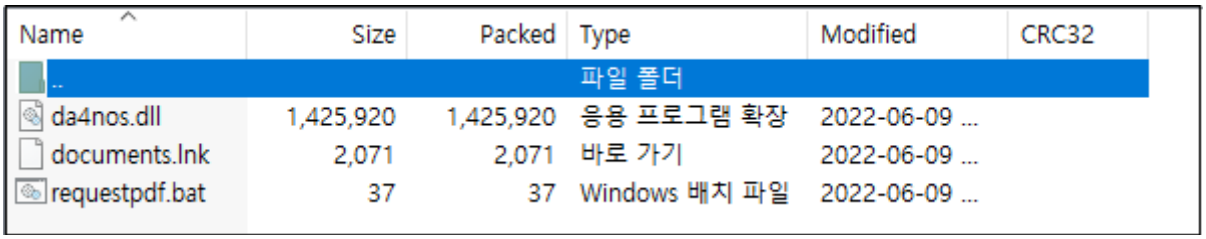
[그림 1] 정상 이메일을 위장하여 범블비 악성코드를 유포하는 피싱 메일

이번 공격은 휴대폰 교체를 이유로 계정 리셋 및 패스워드 초기화를 요청하는 악성 메일을 통해 시도 되었으며, 악성메일에는 첨부파일이 포함되어 있습니다.

주목할만한 점은, 기존에 이메일을 주고 받았었던 관련자의 계정을 사용하여 기존에 주고받았던 정상 이메일에 회신 형식으로 발송했다는 점입니다. 이러한 방식을 통하여 좀 더 효과적으로 수신자를 속여 첨부파일을 실행하도록 유도합니다.

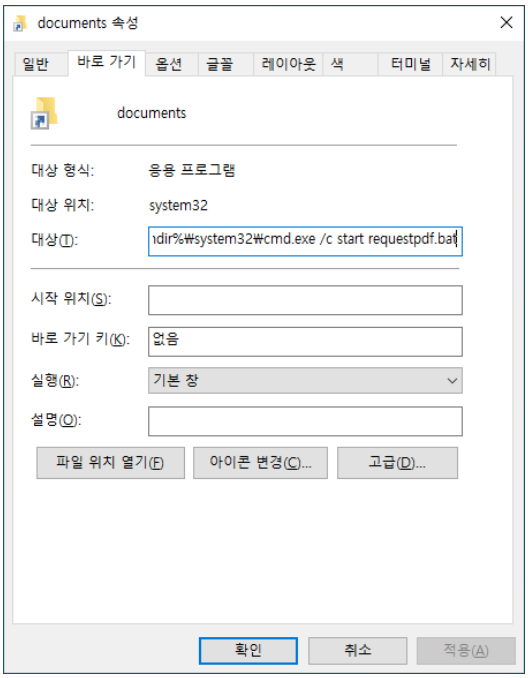


[그림 2] 피싱 메일 내 첨부파일

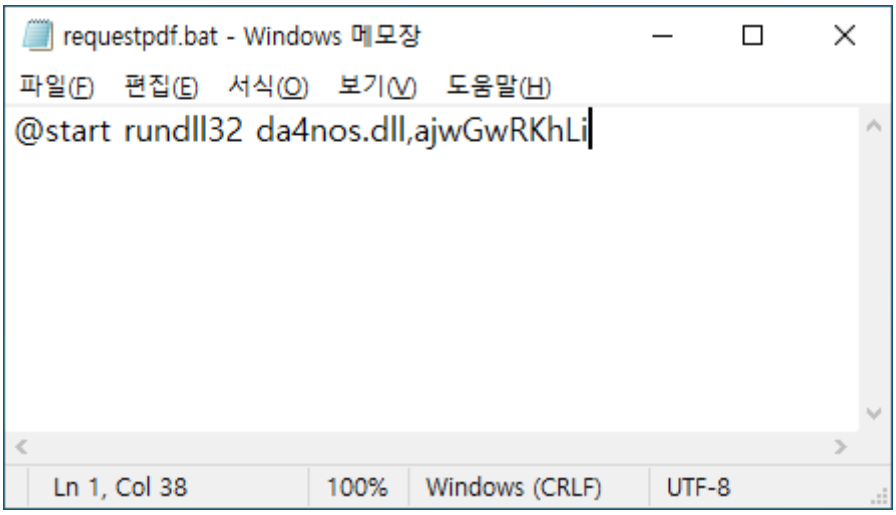


Name	Size	Packed	Type	Modified	CRC32
..			파일 폴더		
da4nos.dll	1,425,920	1,425,920	응용 프로그램 확장	2022-06-09 ...	
documents.lnk	2,071	2,071	바로 가기	2022-06-09 ...	
requestpdf.bat	37	37	Windows 배치 파일	2022-06-09 ...	

[그림 3] iso 파일 내 포함되어 있는 악성파일들



[그림 4] documents.lnk 파일



[그림 5] requestpdf.bat 파일

iso 파일 내에는 dll 파일, lnk 파일 및 bat 파일이 포함되어 있습니다. lnk 파일을 실행하면 지정된 명령어 %windir%\system32\cmd.exe /c start requestpdf.bat를 통해 .bat 파일이 실행되며, requestpdf.bat 파일이 실행되면 da4nos.dll 파일을 실행되며 범블비 악성코드가 실행됩니다.

범블비 악성코드가 실행되면 C&C 서버에 접속하여 추가로 악성코드를 내려 받습니다. 범블비 악성코드는 2022년 3월 등장한 악성코드로, 지속적으로 개발단계에 있는 것으로 추정됩니다.

▶ 참고: 여러 공격자가 사용하는 새로운 악성코드 로더인 Bumblebee 발견

범블비를 유포하는 피싱 메일의 경우, 이메일을 주고받은 적이 있는 사용자의 계정과 기존 이메일에 답장 형식으로 발송하기 때문에 사용자들이 쉽게 속을 수 있습니다.

사용자 여러분들께서는 이메일 내 첨부파일 실행 시 주의를 기울이시기 바라며, 기존에 이메일을 주고받은 적이 있는 사용자라고 하더라도 한번 더 확인하는 습관을 기르셔야 하겠습니다.

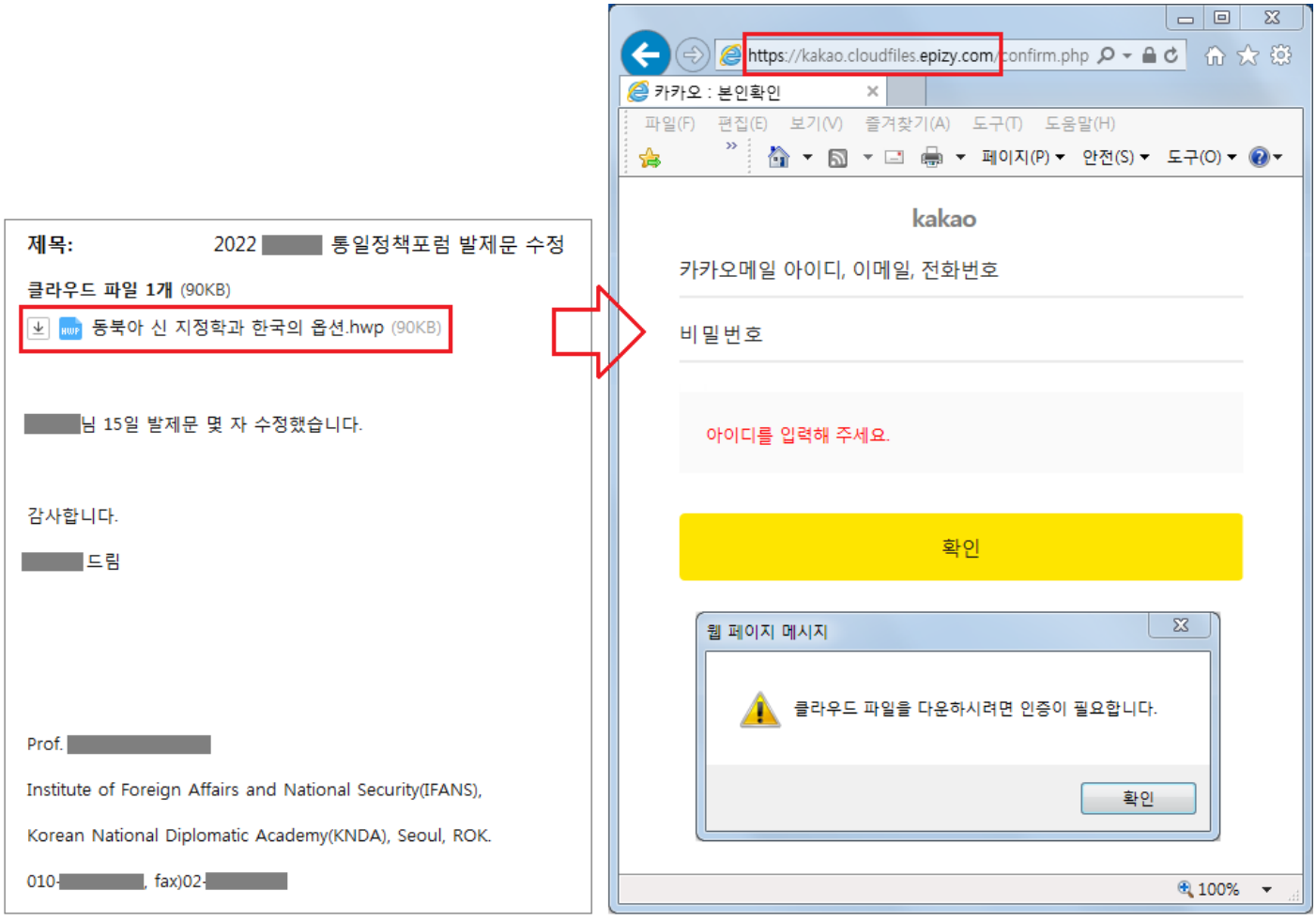
현재 알약에서는 해당 악성코드에 대하여 Trojan.Agent.Bumblebee, Trojan.Agent.LNK.Gen로 탐지 중에 있습니다.

2. 6·15 남북공동선언기념 통일정책포럼 발제문으로 위장한 北 연계 해킹 주의

6·15 남북공동선언 22주년 통일정책포럼 발제문처럼 위장한 해킹 공격이 발견돼 관계자 여러분들의 각별한 주의가 요구됩니다.

이번 공격은 새 정부의 대북통일정책 방향을 진단하고 남북 평화를 모색하기 위해 준비된 통일정책포럼 관련 내용처럼 위장하고 있습니다. 공격자는 전형적인 이메일 피싱 수법을 활용하여 '동북아 신 지정학과 한국의 옵션.hwp' 문서가 클라우드 첨부파일로 있는 것처럼 화면을 구성했고, 실제 포럼 행사에 발표자로 참석하는 국립외교원 외교안보연구소 교수가 보낸 것처럼 사칭했습니다.

해당 포럼은 실제로 6월 15일 한국프레스센터에서 개최되며, 외교·안보·통일 및 대북 분야 전문가들이 발표 및 토론자로 참여할 예정입니다.



[그림 1] 피싱 메일 및 피싱 사이트

만약 수신자가 해당 첨부파일을 클릭하면 해외에 구축된 피싱 사이트가 나타나고, [클라우드 파일을 다운하시려면 인증이 필요합니다.]라는 안내 메시지를 띄어줌으로써 피해자들의 의심을 낮추고자 시도합니다. 또한 사용 중인 포털 계정정보 입력을 유도하여 계정정보 탈취를 시도합니다.

피싱 사이트로 사용된 'kakao.cloudfiles.epizy[.]com' 주소는 얼핏 보기에 포털 클라우드 첨부파일 링크로 무심코 넘길 수 있지만, 자세히 살펴보면 전혀 무관하다는 것을 금방 알 수 있습니다. 피싱에 사용된 'epizy[.]com' 도메인은 '인피니티프리'로 알려진 해외 무료 웹 호스팅 서비스 주소로 북한 연계 피싱 공격 사례에서 지속적으로 발견되고 있습니다.

이번 피싱 주소와 유사한 형태로는 'naver.cloudfiles.epizy[.]com', 'snu.cloudfiles.epizy[.]com', 'korea.onedviver.epizy[.]com', 'yonsei.onedviver.epizy[.]com' 등이 발견된 바 있습니다.

주로 국내 포털 회사나 특정 대학교의 도메인처럼 사칭한 것이 대표적으로, 대학교 주소처럼 위장한 경우 주로 외교·안보·통일 분야 강단에서 활동하는 교수진의 이메일을 집중 공격 한 것으로 드러났습니다.


동북아 신 지정학과 한국의 옵션.hwp
로그인
동북아 신 지정학과 한국의 옵션
1. 한국의 미래 외교안보노선에 대한 고민
ㅇ 오늘 국제체제는 냉전기 양극체제, 탈냉전 초기 미국 패권의 단극체제와 질적으로 다른 다극 또는 무극체제의 양상을 보이며, 강대국 세력경쟁이 전개되고 있음.
- 한국은 전통적으로 미국의 동맹국이지만 오늘 국제체제의 극적인 변동을 촉발한 중국과 지리적으로 근접해 있고 정치·경제적으로 긴밀한 관계를 유지하여 온 바, 최근 미중 전략경쟁의 악화로 국내에서 한국의 외교안보노선을 둘러싼 논쟁이 분분함.
- 미중 전략경쟁이 전 공간과 분야로 확장되고 심화되면서 한국에 대한 양자택일의 압박이 증가함에 따라, 종래 한국의 미중관계 대응전략으로 알려진 '안미경중(安美經中)'과 '전략적 모호성'은 그 효용을 다했으며, 새로운 대응전략이 시급하게 필요함.
ㅇ 한국민은 민주화와 선진화 달성, 세계 10대 경제대국, "30-50클럽"에 7번째 진입 등의 높아진 국력과 자긍심에 상응하는 새로운 외교안보 전략을 요구하고 있음.
- 새로운 외교안보 환경에 대응하기 위해 국민과 정치권은 한국 외교가 보다 국익에 충실하고, 전략적이며, 원칙에 기반한 외교(국익외교·전략외교·원칙외교)를 추진할 것을 주문하고 있음.
그런데 정부와 전문가들은 아직 국민과 정치권이 공감하는 국익, 전략, 원칙의 내용을 제대로 제시하지 못하고 있는 실정임.
ㅇ 그동안 한국은 미국의 동맹국이자 자유진영국가로서 미국의 보호와 지원 아래서 고도 경제성장에 성공했고 국력이 크게 신장되었지만, 냉전의 보호망과 미국 패권이 사라진 후 한국은 매 순간 외교안보적 선택을 해야 하고, 그 결과도 감당해야 함.
- 오늘 한국은 최악의 안보구조를 가진 분단국이자, 미중 간 지정학적 경쟁에 '끼인 국가'로서 악화된 외교안보 환경 속에서도 지속적인 평화 번영을 보장하기 위한 보다 효과적인 외교안보전략이 필요함.
12페이
ㅇ 미중 전략경쟁 시대 한국 외교안보전략 대한 기존 연구과 제안

[그림 2] 피싱 공격 후 보여지는 정상 문서 화면

만일 피해자가 계정정보 입력을 한다면, 이 후 특정 구글드라이브 주소로 변경하여 정상 문서를 보여주어 해킹 공격임을 인지하지 못하도록 합니다.

주목할 점은 최근 이와 유사한 공격에서 발견된 악성 및 정상 문서들의 마지막 저장 정보에 'kisa' 이름이 공통으로 사용되었다는 사실인데, 'kisa' 이름이 사용된 여러 위협 사례들이 전부 북한 소행으로 지목된 페이크 스트라이커 캠페인과 정확히 일치하고 있어 ESRC에서는 현재 어떤 의도를 가진 공격인지 면밀한 관찰과 조사중에 있습니다.

최근 들어 악성 DOC나 HWP OLE 기반의 지능형지속위협(APT) 공격이 증가 추세를 보이고 있으며, 이 가운데 대용량 파일이나 클라우드 기반 첨부파일처럼 조작한 이메일 피싱도 꾸준히 보고되고 있습니다.

뿐만 아니라, 해외 무료 웹 호스팅을 악용한 공격은 이미 수년 전부터 계속 진행 중이며, 주로 북한이 연계된 '페이크 스트라이커' 위협 캠페인에서 발견되고 있습니다. 이들은 '인피니티프리' 외에도 다양한 도메인 주소를 제공하는 '웹프리호스팅'이라는 해외 서비스도 번갈아 가면서 사용 중입니다.

6월에도 北 소행으로 지목된 사이버 안보위협은 외교·안보·통일·국방 분야를 넘어 특정 분야에 종사하는 민간인까지 꾸준히 이어지고 있으며, 특히 안드로이드 기반 스마트폰 이용자를 노린 북한 배후 모바일 공격까지 보고되고 있어, 기업 및 기관뿐만 아니라 일반 사용자들 역시 유사한 보안위협에 노출되지 않도록 더 많은 관심과 주의가 필요합니다. 한편, 이스트시큐리티 ESRC는 이와 관련된 사이버 위협 정보를 한국인터넷진흥원(KISA) 등 관계 당국과 긴밀히 공유해 기존에 알려진 위협이 확산되지 않도록 협력을 유지하고 있습니다.

3

악성코드 분석 보고

[Trojan.MSIL.Stealer.gen] 악성코드 분석 보고서

세인트스틸러(Saintstealer)는 이름에서 알 수 있듯이 인포스틸러(Infostealer) 악성코드로 여러 웹 브라우저와 다양한 프로그램의 계정 정보 및 하드웨어 정보, 특정 파일 등을 탈취하는 기능을 가지고 있다.

이렇게 수집된 모든 정보를 취합하여 압축 파일로 만들어 텔레그램 봇을 이용하여 공격자에게 전송하며, 추가 메타 데이터는 공격자가 지정한 C&C 주소로 전송하는 특징을 가지고 있다.

또한, 진단을 우회하기 위해 주로 닷넷(.NET) 프로그램의 형태로 유포되고 있다.

```
int width = Screen.PrimaryScreen.Bounds.Width;
int height = Screen.PrimaryScreen.Bounds.Height;
Bitmap bitmap = new Bitmap(width, height);
Graphics graphics = Graphics.FromImage(bitmap);
graphics.CopyFromScreen(0, 0, 0, 0, bitmap.Size);
MemoryStream memoryStream = new MemoryStream
{
    Position = 0L
};
graphics.InterpolationMode = InterpolationMode.Bicubic;
graphics.PixelOffsetMode = PixelOffsetMode.HighSpeed;
graphics.SmoothingMode = SmoothingMode.HighSpeed;
bitmap.Save(memoryStream, ImageFormat.Jpeg);
byte[] image;
if ((image = ((memoryStream != null) ? memoryStream.ToArray() : null)) == null)
{
    image = (memoryStream.GetBuffer() ?? null);
}
Program.image = image;
```

[그림] 스크린 캡쳐 코드 중 일부

세인트스틸러(Saintstealer)는 Chromium기반 브라우저의 패스워드, 쿠기 및 자동채움 폼(Autofill) 데이터 정보와 디스코드, 텔레그램과 같은 다양한 프로그램 정보도 탈취 기능을 가지고 있다.

세인트스틸러는 사용자 정보를 탈취하는 것을 주목적으로 하며, 민감한 사용자 계정 정보를 탈취하기 때문에 추가적인 피해가 야기될 수 있어 각별한 주의가 필요하다.

최근에 새롭게 등장한 악성코드는 주로 다크넷(Darknet) 시장에서 구독 서비스 형태로 다양한 해킹 관련 프로그램들과 함께 거래되고 있다.

따라서, 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 확인을 지양해야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

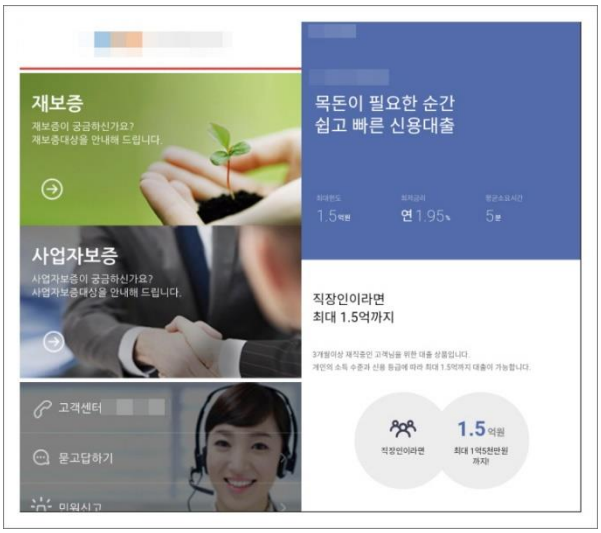
현재 알약에서는 **'Trojan.MSIL.Stealer.gen'** 으로 진단하고 있다.

[Trojan.Android.Banker] 악성코드 분석 보고서

보이스피싱은 꾸준하게 발생하고 있으며 꼭 전화를 통한 방법이 아닌 메신저를 활용한 방법들도 증가하고 있다. 여러 가지 사례들이 확인되고 있지만 아래와 같이 분류할 수 있다.

1. 각종 기관을 사칭하는 방법
   A. 검사나 경찰, 은행원을 사칭하여 피해자에게 문제가 생긴 것처럼 얘기하고 해결을 위한 돈을 요구
2. 메신저를 통해 지인과 가족을 사칭한 방법
   A. 휴대폰이 망가져서 친구 계정으로 연락했다며 수리비가 급하니 돈을 요구
3. 연락처에 저장된 가족 번호를 활용한 방법
   A. 010을 제외한 뒤 번호 8자리를 가지고 연락처의 이름을 판단하는 점을 악용해 가족이나 지인으로 위장하여 돈을 요구
4. 대출을 받기 위한 신용 조회 방법
   A. 취업자 또는 소상공인들을 상대로 저금리 대출을 해준다며 신용 등급을 높이기 위한 돈을 요구

이 중에서도 대출과 관련된 악성 앱이 자주 발견되고 있으며 위장하는 수법이 날이 갈수록 점점 교묘해지고 있다.



[그림] 유사 앱 화면

해당 공격자의 경우 다양하게 위장할 수 있도록 이미 웹 페이지를 이미지와 함께 구현해 두었다. 은행을 비롯한 공공기관까지 범위는 넓으며 실제 입력 폼과 신청, 접수 완료 메시지 등을 표시하고 있으므로 스마트폰 사용자는 구별하기 힘들 수 있다. 따라서 출처가 불분명한 앱은 설치하지 않도록 각별한 주의가 요구된다.

현재 알약M에서는 해당 앱을 **'Trojan.Android.Banker'** 탐지 명으로 진단하고 있다.

4

글로벌 보안 동향

‘Follina’ 제로데이 취약점, 오피스 이전 버전 위험에 빠트려

Zero-Day ‘Follina’ Bug Lays Older Microsoft Office Versions Open to Attack

공격자가 Microsoft Office에 존재하는 제로데이 취약점을 악용하여 원격 Word 템플릿 기능을 통해 타깃 시스템에서 악성코드를 실행 가능한 것으로 나타났습니다.

이는 지난 주말 일본의 보안업체인 Nao Sec이 트위터에 제로데이에 대한 경고를 발행해 알려졌습니다.

유명 보안 연구원인 Kevin Beaumont는 해당 제로데이의 코드가 이탈리아 기반의 지역 번호인 Follina – 0438을 참조하기 때문에 취약점을 "Follina"라 명명했다고 밝혔습니다.

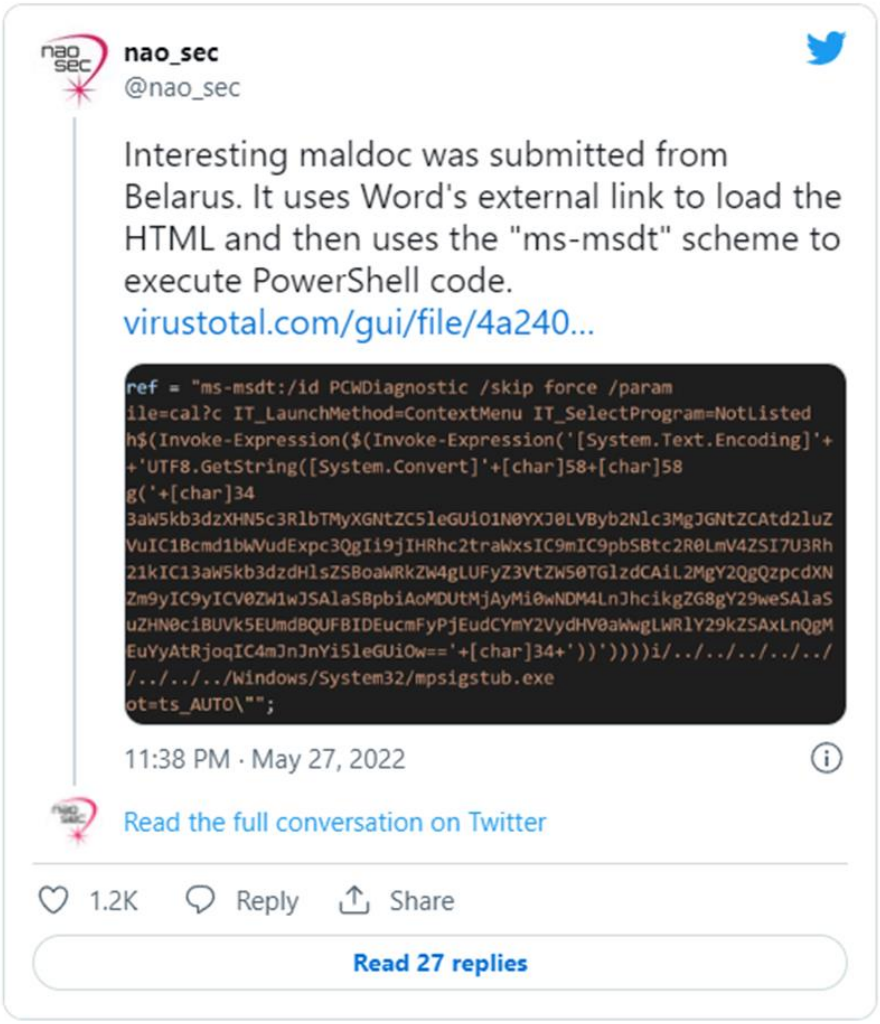
Beaumont는 이 취약점이 Microsoft Word의 원격 템플릿 기능을 악용하고 있으며, Office 기반 공격에서 흔히 발견되는 일반적인 매크로 기반 익스플로잇 공격을 사용하지 않는다고 밝혔습니다. Nao Sec은 해당 버그의 라이브 샘플은 Word 문서 템플릿과 벨로루시의 인터넷 프로토콜(IP) 주소에 대한 링크에서 발견되었다고 설명했습니다.

공격자들이 이 제로데이 취약점을 활발히 악용했는지 여부는 알 수 없습니다. 확인되지는 않았지만, PoC 코드가 존재하고 더욱 최신 버전의 Office가 공격에 취약하다는 보고서가 있습니다.

한편, 보안 연구원은 사용자가 패치 대신 Microsoft 공격 노출 영역을 감소하는 조치를 취해 이 공격의 위험을 완화시킬 수 있다고 설명했습니다.

Follina의 작동 방식

Nao Sec의 연구원들은 원격 서버에서 HTML(Hypertext Markup Language) 파일을 통해 익스플로잇을 로드하는 악성 템플릿이 감염 경로에 포함된다고 설명했습니다.



[이미지 출처] https://twitter.com/nao_sec/status/1530196847679401984>

[출처]
https://threatpost.com/zero-day-follina-bug-lays-older-microsoft-office-versions-open-to-attack/179756/
https://twitter.com/nao_sec/status/1530196847679401984 (IOC)

REvil 랜섬웨어의 새로운 샘플 발견, 활동 재개설 확인돼

REvil ransomware returns: New malware sample confirms gang is back

러시아와 미국 사이의 긴장이 고조되고 있는 가운데, 악명 높은 REvil 랜섬웨어가 다시 활동을 재개했습니다. 새로운 버전은 새로운 인프라와 개선된 암호화기를 통해 표적화된 공격이 가능해졌습니다.

지난 10월 법 집행 기관이 REvil 랜섬웨어의 Tor 서버를 압수한 후 러시아의 법 집행 기관이 그룹의 멤버를 체포하여 활동을 중단했습니다.

하지만, 러시아는 우크라이나 침공 이후 미국이 REvil 그룹에 대한 협상 과정을 포기하고 관련된 통신 채널을 폐쇄했다고 밝힌 바 있습니다.

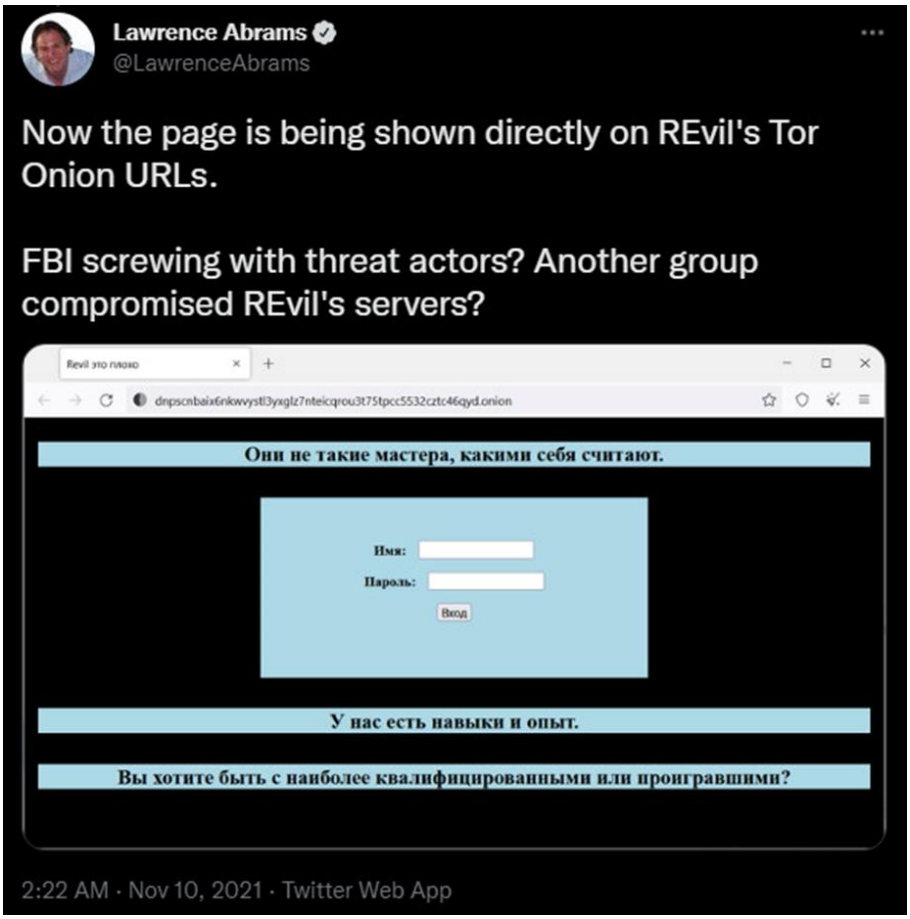
다시 살아난 REvil의 Tor 사이트

이후 얼마 지나지 않아, 기존 REvil의 Tor 인프라가 다시 작동하기 시작했습니다. 하지만 방문자에게 이전 웹사이트를 보여주는 대신 이름이 없는 새로운 랜섬웨어 작업을 위한 URL로 이동시켰습니다.

이 사이트는 예전 REvil의 웹사이트와 전혀 다른 것처럼 보이지만, 기존 인프라가 새로운 사이트로 리디렉션되고 있기 때문에 REvil이 다시 운영될 가능성이 있을 것으로 추측할 수 있습니다. 게다가, 새로운 사이트에는 이전 REvil 공격을 통해 훔친 데이터와 새로운 피해자의 데이터가 섞인 채 게시되어 있었습니다.

이러한 증거가 REvil 랜섬웨어가 이름이 없는 새로운 브랜드로 변경했음을 명백히 보여주고 있지만, 해당 Tor 사이트는 지난 11월 "REvil은 나쁘다"는 메시지를 표시하기도 했습니다.

하지만 Tor 사이트에는 다른 공격자나 법 집행 기관 또한 접근이 가능했기 때문에 해당 웹 사이트만으로 해킹 그룹이 다시 활동을 재개했다는 충분한 증거가 되지는 못했습니다.



[그림] 안티 REvil 메시지를 표시하는 REvil의 Tor 사이트

[이미지 출처] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

REvil이 실제로 활동을 재개했는지 확실히 확인할 수 있는 유일한 방법은 해당 랜섬웨어 암호화기의 샘플을 분석하여 패치되었는지, 소스코드에서 컴파일되었는지 확인하는 것이었습니다.

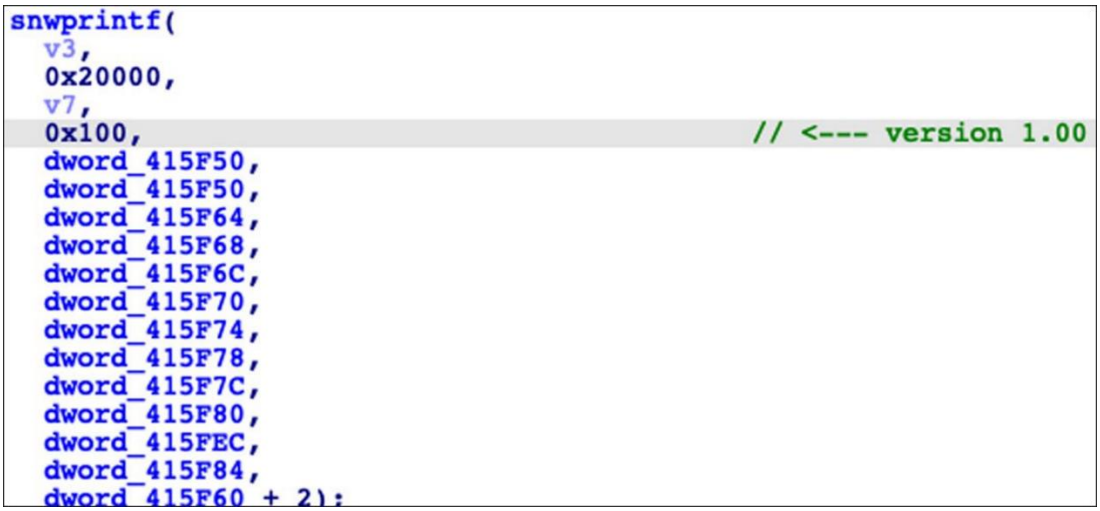
하지만 이번 주 AVAST의 연구원인 Jakub Kroustd이 새로운 랜섬웨어의 암호화기 샘플을 발견해 새로운 작전이 REvil과 실제로 관련이 있음을 확인했습니다.

랜섬웨어 샘플로 활동 재개 확인해

몇몇 랜섬웨어 작업이 REvil의 암호화기를 사용하고 있지만, 이들 모두 그룹의 소스코드에 직접적으로 접근하기보다는 패치된 실행파일을 사용합니다.

하지만, 여러 보안 연구원과 악성코드 분석가들은 새로운 작업에 사용된 REvil 샘플이 소스코드를 통해 컴파일되었으며 새로운 변경 사항이 포함된 것을 발견했다고 전했습니다.

보안 연구원인 R3MRUM은 트위터를 통해 REvil의 샘플의 버전 번호가 1.0으로 변경되었지만, 종료되기 전 REvil에서 공개한 마지막 버전인 2.08의 연속이라고 밝혔습니다.



[그림] 새로운 REvil 암호기의 버전 변경

[이미지 출처] https://twitter.com/R3MRUM/status/1520195427068350464

연구원은 해당 암호화기가 실제로 파일을 암호화하지 않는 이유를 설명할 수는 없었지만, 소스코드를 통해 컴파일된 것으로 추측된다고 밝혔습니다.

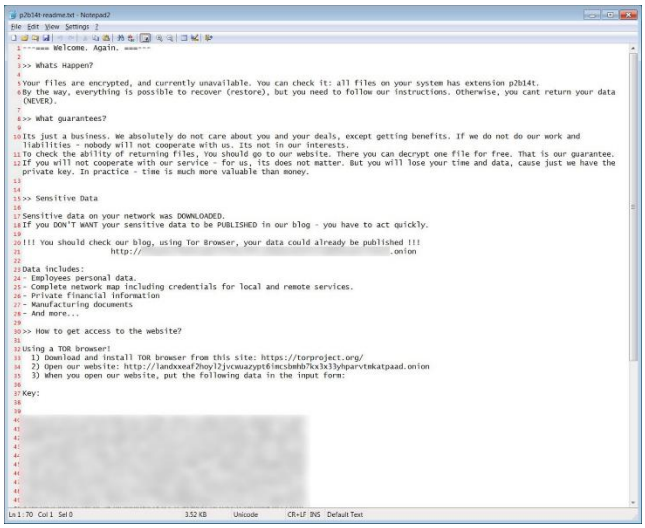
Advanced Intel의 CEO인 Vitali Kremez 또한 REvil의 새로운 샘플을 역설계한 결과, 지난 4월 26일 소스코드에서 컴파일되었으며 이후 패치되지 않았음을 확인했다고 밝혔습니다.

Kremez는 새로운 REvil 샘플에 새로운 구성 필드인 'accs'가 추가되었다고 밝혔습니다. 이 필드에는 공격을 통해 노리는 특정 피해자의 크리덴셜이 포함되어 있습니다.

Kremez는 해당 'accs' 구성 옵션이 고도의 타깃화된 공격을 위해 특정 계정과 윈도우 도메인을 포함하지 않는 다른 기기가 암호화되는 것을 방지하기 위한 것이라 추측했습니다.

'accs' 옵션 이외에도, 새로운 REvil 샘플의 구성에서는 캠페인 및 제휴 식별자로 사용되는 SUB 및 PID 옵션을 수정해 '3c852cc8-b7f1-436e-ba3b-c53b7fc6c0e4'와 같은 더욱 긴 GUID 유형 값을 사용합니다.

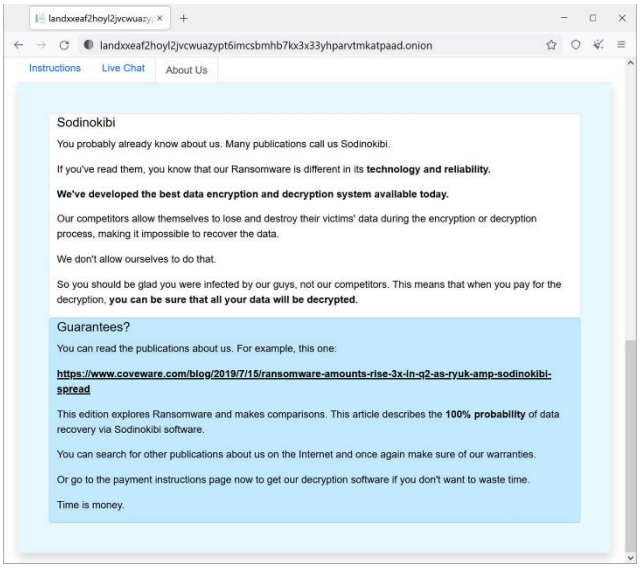
BleepingComputer에서 랜섬웨어 샘플을 테스트한 결과, 이는 파일을 암호화하지는 않았지만 REvil의 이전 랜섬노트와 유사한 노트를 생성했습니다.



[그림] REvil의 랜섬노트

[이미지 출처] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/>

또한 기존 REvil 사이트와 리브랜딩된 사이트에는 약간의 차이가 있지만, 피해자가 사이트에 로그인할 경우에는 이전 사이트와 거의 동일한 것으로 나타났습니다. 또한 공격자는 아래와 같이 'Sodinokibi'라 주장하고 있었습니다.



[그림] Sodinokibi라 주장하는 새로운 랜섬웨어

[이미지 출처] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/>

'Unknown'으로 알려진 REvil의 대표는 아직까지 찾을 수 없었지만, 위협 인텔리전스 연구원인 FellowSecurity는 BleepingComputer 측에 REvil의 이전 핵심 개발자 중 한 명이 랜섬웨어 작전을 다시 실행했다고 전했습니다.

그가 핵심 개발자였기 때문에 REvil의 소스코드 전체 및 이전 사이트의 Tor 개인 키에 잠재적으로 접근이 가능했던 것으로 추측해볼 수 있습니다.

[출처]
https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/
https://twitter.com/R3MRUM/status/1520195427068350464
https://twitter.com/JakubKroustek/status/1520135975262957568 (IOC)

크립토마이너로 윈도우 및 리눅스 시스템을 하이재킹하는 새로운 Sysrv 봇넷 발견

New Sysrv Botnet Variant Hijacking Windows and Linux with Crypto Miners

마이크로소프트가 윈도우 및 리눅스 시스템에 코인 마이너를 설치하기 위해 웹 애플리케이션 및 데이터베이스의 보안 취약점 다수를 악용하는 새로운 srv 봇넷 변종에 대해 경고했습니다.

새 버전은 Sysrv-K라 명명되었으며, 이는 웹 서버를 제어하기 위해 일련의 익스플로잇을 무기화합니다. 이 크립토재킹 봇넷은 2020년 12월 처음으로 등장했습니다. 마이크로소프트는 트위터를 통해 아래와 같이 밝혔습니다.

"Sysrv-K는 인터넷을 스캔해 다양한 취약점이 존재하는 웹 서버를 찾아 자기 자신을 스스로 설치합니다."
"취약점은 경로 탐색, 원격 파일 유출, 임의 파일 다운로드, 원격 코드 실행 등 범위가 넓습니다."

해당 취약점에는 악성 요청을 통해 원격 호스트에서 임의 원격 실행을 허용하는 Spring Cloud Gateway의 코드 삽입 취약점인 CVE-2022-22947(CVSS 점수: 10.0) 또한 포함됩니다.

CVE-2022-22947이 실제 공격에서 악용되어 미 CISA에서는 해당 취약점을 알려진 악용 취약점 카탈로그에 추가했습니다.

Sysrv-K의 주요 차이점은 WordPress의 구성 파일과 해당 백업을 검색해 데이터베이스 크리덴셜을 가져온 다음 웹 서버를 가로채는 데 사용한다는 것입니다. 또한 이는 Telegram Bot을 활용하기 위해 C2 통신 기능을 업그레이드했다고 밝혔습니다.

일단 감염되면, 이는 피해자 시스템에서 사용 가능한 SSH 키를 통해 측면 이동을 실행하며 악성코드의 복사본을 또 다른 시스템에 배포하고 봇넷의 크기를 확장시켜 효과적으로 전체 네트워크를 위험에 빠뜨립니다.

지난 해, Lacework Labs 연구원은 이와 관련하여 아래와 같이 밝혔습니다.

"Sysrv 악성코드는 이미 알려진 취약점을 악용하여 크립토재킹 악성코드를 확산시킵니다."
"공격자가 시스템을 해킹하는 것을 막기 위해서는 공개된 애플리케이션의 보안 패치가 최신 상태로 유지되어야 합니다."

마이크로소프트는 조직이 인터넷에 노출된 서버를 보호하는 것 이외에도 적시에 보안 업데이트를 적용하고 크리덴셜을 보호하여 위험을 줄이도록 권고했습니다.

[출처]
https://thehackernews.com/2022/05/new-sysrv-botnet-variant-hijacking.html
https://www.lacework.com/blog/sysrv-hello-expands-infrastructure/ (IOC)
https://tanzu.vmware.com/security/cve-2022-22947

마이크로소프트, 안드로이드 기기 수백만 대에 사전 설치된 앱에서 치명적인 취약점 발견

Microsoft Finds Critical Bugs in Pre-Installed Apps on Millions of Android Devices

안드로이드 시스템에 수백만 회 이상 선 설치된 프레임워크에서 심각도 높은 취약점 4개가 발견되었습니다.

현재 이스라엘 개발자인 MCE Systems에서 수정된 이 문제는 잠재적으로 공격자가 원격 및 로컬 공격을 수행하거나 광범위한 시스템 권한을 활용해 민감 정보를 얻기 위한 벡터로 악용할 수 있었습니다.

마이크로소프트 365 디펜더 연구팀은 지난 금요일 보고서를 발표해 아래와 같이 밝혔습니다.

"요즘 안드로이드 기기 대부분과 함께 제공되는 사전 설치 또는 기본 애플리케이션이 많습니다. 때문에 취약한 일부 앱은 루트 액세스 권한 없이는 기기에서 완전히 제거하거나 비활성화할 수 없습니다."

이 취약점은 명령 주입, 로컬 권한 상승 등이며 CVE-2021-42598, CVE-2021-42599, CVE-2021-42600, CVE-2021-42601으로 등록되었습니다. CVSS 점수는 7.0 ~ 8.9사이입니다.

```
public void executeSystemCloseProcess(short paramShort, JSONArray paramJSONArray,
    Logger.log("[ExecuteInternal] Executing Close Process", new Object[0]);
    Types.ErrorCode errorCode = Types.ErrorCode.generalError;
    JSONObject jSONObject1 = new JSONObject();
    JSONObject jSONObject2 = new JSONObject();
    try {
      Types.ErrorCode errorCode1;
      String str1 = paramJSONArray.getJSONObject(0).getString("value").trim();
      Shell shell = Shell.getInstance();
      StringBuilder stringBuilder = new StringBuilder();
      stringBuilder.append("am force-stop \"");
      stringBuilder.append(str1);
      stringBuilder.append("\"");
      String str2 = shell.SendCommand(stringBuilder.toString());
```

[그림] 명령 주입 PoC 익스플로잇 코드

[이미지 출처] https://www.microsoft.com/security/blog/2022/05/27/android-apps-with-millions-of-downloads-exposed-to-high-severity-vulnerabilities/

```
send_request(service, command, data)
{
    console.log("sploit.send_request(): called");

    // Create a new context
    var context = this.create_guid();

    // Build the JSON request
    var json_req = {
            "context": context,
            "service": service,
            "request": {
                "command": command,
                "data": data
            },
            "client": {
                "id": this.create_guid()
            }
        };
    var json_req_string = JSON.stringify(json_req);

    // Save the context for the response and invoke the request
    this.contexts.set(context, json_req_string);
    console.log("sploit.send_request(): sending request " + json_req_string);
    window.AndroidWebViewBridge.request(json_req_string);
}
```

[그림] WebView에 유사한 JavaScript 코드 삽입

[이미지 출처] https://www.microsoft.com/security/blog/2022/05/27/android-apps-with-millions-of-downloads-exposed-to-high-severity-vulnerabilities/

해당 취약점은 2021년 9월에 발견 및 보고되었으며, 아직까지 취약점이 악용되고 있다는 증거는 찾아볼 수 없었습니다.

Microsoft는 문제의 취약한 프레임워크를 사용하는 앱의 전체 목록을 공개하지는 않았습니다. 이 프레임워크는 안드로이드 기기에 영향을 미치는 문제를 식별하고 수정하는 자가 진단 메커니즘을 제공하도록 설계되었습니다.

이는 프레임워크가 기능을 수행하기 위해 오디오, 카메라, 전원, 위치, 센서 데이터, 스토리지를 포함한 광범위한 액세스 권한을 가지고 있음을 의미합니다. Microsoft는 공격자가 영구적인 백도어를 삽입하고 제어권을 얻는 것도 가능할 수 있다고 밝혔습니다.

영향을 받는 앱 중 일부는 Telus, AT&T, Rogers, Freedom Mobile, Bell Canada와 같은 대규모 국제 모바일 서비스 제공업체에서 사용하는 앱입니다.

Mobile Klinik Device Checkup (com.telus.checkup)
Device Help (com.att.dh)
MyRogers (com.fivemobile.myaccount)
Freedom Device Care (com.freedom.mlp.uat),
Device Content Transfer (com.ca.bell.contenttransfer)

또한 Microsoft는 사용자에게 "com.mce.mceiotraceagent" 앱 패키지(휴대폰 수리점에서 설치한 것으로 추정되는 앱)를 찾아보고 발견될 경우 기기에서 제거할 것을 권장했습니다.

취약한 앱은 사전 설치되기도 하지만 구글 플레이 스토어에서도 다운 가능하며, 프로세스에서 이러한 문제를 찾도록 설계되지 않았기 때문에 앱 스토어의 자동 안전 검사를 통과한 것으로 나타났습니다.

[출처]
https://thehackernews.com/2022/05/microsoft-finds-critical-bugs-in-pre.html
https://www.microsoft.com/security/blog/2022/05/27/android-apps-with-millions-of-downloads-exposed-to-high-severity-vulnerabilities/

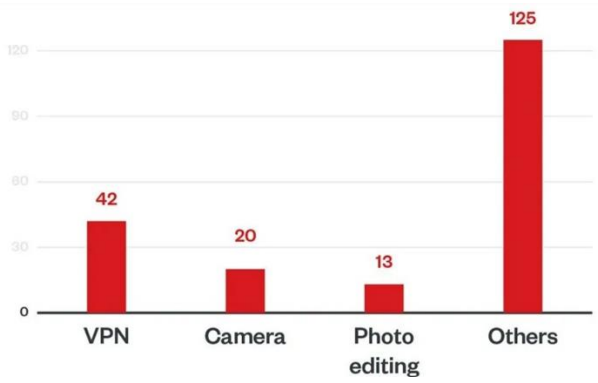
플레이 스토어의 앱 200개 이상, Facestealer 인포 스틸러 배포해

Over 200 Apps on Play Store were distributing Facestealer info-stealer

Trend Micro의 연구원들이 플레이 스토어에서 안드로이드 앱 200개 이상을 통해 감염된 안드로이드 기기에서 민감 데이터를 훔치는 스파이웨어인 Facestealer가 배포되는 것을 발견했습니다. 해당 악성 앱은 크리덴셜, 페이스북 쿠키, 기타 개인 식별 정보 등을 탈취합니다.

전문가들이 발견한 악성 앱 중 일부는 수십만 회 이상 설치되었습니다.

Facestealer 스파이웨어는 2021년 7월 Dr. Web 연구원에 의해 처음으로 발견되었으며 해당 악성코드의 개발 팀은 코드를 빈번히 업데이트했습니다.



[이미지 출처] https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html>

악성 앱의 대부분은 VPN 소프트웨어(42개), 카메라(20개), 사진 편집(13개) 앱이었습니다.

또한 Trend Micro의 연구원들은 2021년 8월에 발견했던 변종과 유사한 가짜 가상 화폐 채굴 앱 40개를 발견했습니다. 해당 앱은 사용자가 유료 서비스를 구독하거나 광고를 클릭하도록 속입니다.

Trend Micro는 보고서를 통해 아래와 같이 밝혔습니다.

"Facestealer 앱은 VPN(가상 사설망), 카메라, 사진 편집, 피트니스 앱 등 간단한 툴로 위장한 매력적인 미끼입니다. 페이스북의 쿠키 관리 정책을 실행하는 방식 때문에 이러한 유형의 앱이 계속해서 구글 플레이를 감염시킬 것이라 추측됩니다."

"가짜 암호화폐 채굴기의 경우 운영자는 피해자를 속여 가짜 클라우드 기반 가상 화폐 채굴 서비스를 구매하게 해 이익을 얻으려고 할 뿐만 아니라 사용자의 개인 키 및 기타 민감 가상 화폐 관련 정보를 수집하려 시도합니다. 이들은 향후 개인 키와 연상 문구를 훔치는 또 다른 수법이 등장할 가능성이 높다고 생각합니다."

[출처]
https://securityaffairs.co/wordpress/131370/malware/facestealer-info-stealer-play-store.html
https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html (IOC)

www.estsecurity.com

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616