이스트시큐리티

보안 동향 보고서

No.136 2021.01

No.136 2021.01

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

12 월에도 '탈륨(Thallium)' '금성 121(Geumseong 121)' 등 북한 연계 조직의 소행으로 추정되는 APT 공격이 연이어 발견됐습니다. 이들은 한국과 미국 등지에서 활동하는 APT 그룹 중 가장 활발한 첩보 활동을 전개하고 있으며 2020 년 한 해 동안 코로나 19 치료제를 연구하는 국내외 대표 제약사, 국내 암호화폐 거래 관계자와 과학기술 분야 교육 관계자 등을 타깃으로 공격을 수행한 것이 확인됐습니다.

12 월 한 달 동안에 발생했던 주목할만한 APT 공격에는 '통일부로 가장한 악성 이메일 공격', '평화 통일 관련 이야기 공모전 신청서를 사칭한 악성 HWP 문서 공격'과 '국내 블록체인 기업 체불확인원 문서로 위장한 악성 DOC 파일 공격'이 있었습니다. 특히 평화 통일 관련 이야기 공모전 신청서를 사칭한 공격에서는 한컴오피스 한글 프로그램의 객체 연결 삽입(OLE) 기능을 악용했는데, 이러한 공격 방식은 문서 파일 차제 취약점을 악용하지 않기 때문에 최신 버전의 프로그램을 사용하거나 보안 업데이트를 모두 적용한 경우에도 악성코드가 실행될 가능성이 크기 때문에 매우 위험합니다. 이와 관련된 자세한 분석 내용은 이스트시큐리티 알약 블로그와 Threat Inside 게시물 [북한 동향정보, 통일 이야기 공모전 문서 사칭… 北 연계 APT 조직 공격 주의보]에서 확인하실 수 있습니다.

이번 달에도 역시 전 세계적으로 관심을 받는 이슈를 악용한 공격이 확인됐습니다. 지난 12 월 10 일 출시된 'Cyberpunk 2077'의 인기를 악용하여 해당 게임의 모바일 버전으로 위장한 안드로이드 랜섬웨어 'CoderWare'가 발견됐습니다. 해당 가짜 모바일 게임은 정식 구글 플레이스토어로 위장한 가짜 웹사이트를 통해 배포되고 있었습니다. 아직까지 CoderWare 랜섬웨어의 복호화 가능 여부는 공식적으로 확인되지 않았습니다. 이렇듯 저작권이 있는 소프트웨어를 무료로 설치하려고 시도할 경우 악성코드에 감염될 위험에 처하게 됩니다. 따라서 소프트웨어나 애플리케이션을 설치할 경우에는 반드시 공식 다운로드 센터 및 앱스토어를 사용해야 합니다.

이스트시큐리티에서는 연말을 맞아 2020 년 한 해 동안 발생한 주요 보안 이슈에는 어떤 것들이 있었는지 되짚어 보며 2021 년에는 어떤 보안 이슈들이 발생할 것인지 전망해보았습니다. 2021 년에는 1) 정부 지원 방식의 고도화된 APT 공격이 지속적으로 등장할 것이며 2) 재택근무 증가에 따라 원격 업무 환경 타깃 공격이 지속되고 3) 랜섬웨어 협박을 통한 금전 갈취 규모가 커지고 지속될 것으로 예상됩니다. 또한 4) 5G 네트워크 사용 증가에 따라 취약점을 악용한 공격이 활발해지고 5) 2020 년과 마찬가지로 사회적 이슈를 악용한 악성 앱 유포 공격이 증가할 것입니다. 이스트시큐리티가 발표한 보안 이슈 결산에 관심이 있으신 분들은 알약 블로그와 Threat Inside 에서 전문을 확인하실 수 있습니다.

2020 년 한 해를 돌아보면 사이버 위협의 수위는 날이 갈수록 높아지고 있고 공격 방식 또한 고도화되고 있습니다. 따라서 2021 년에는 기존에 발생한 위협 사례들을 확인하고 인지하여 철저하게 보안 수칙을 준수하는 노력이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 12 월의 감염 악성코드 Top 15 리스트에서는 지난달 2 위로 1 단계 하락했던 Hosts.media.opencandy.com 이 다시 1 위를 차지했으며 Misc.HackTool.AutoKMS 와 Trojan.ShadowBrokers.A 가 한 계단씩 상승했다. 그 외에 이번 달에는 Gen:Variant.Johnnie.248927 을 비롯한 6 건의 악성코드가 새롭게 Top 15 에 백도어 악성코드 유형에 해당하는 Backdoor.Generic.792814 가 6 계단 급상승한 모습을 보였다.

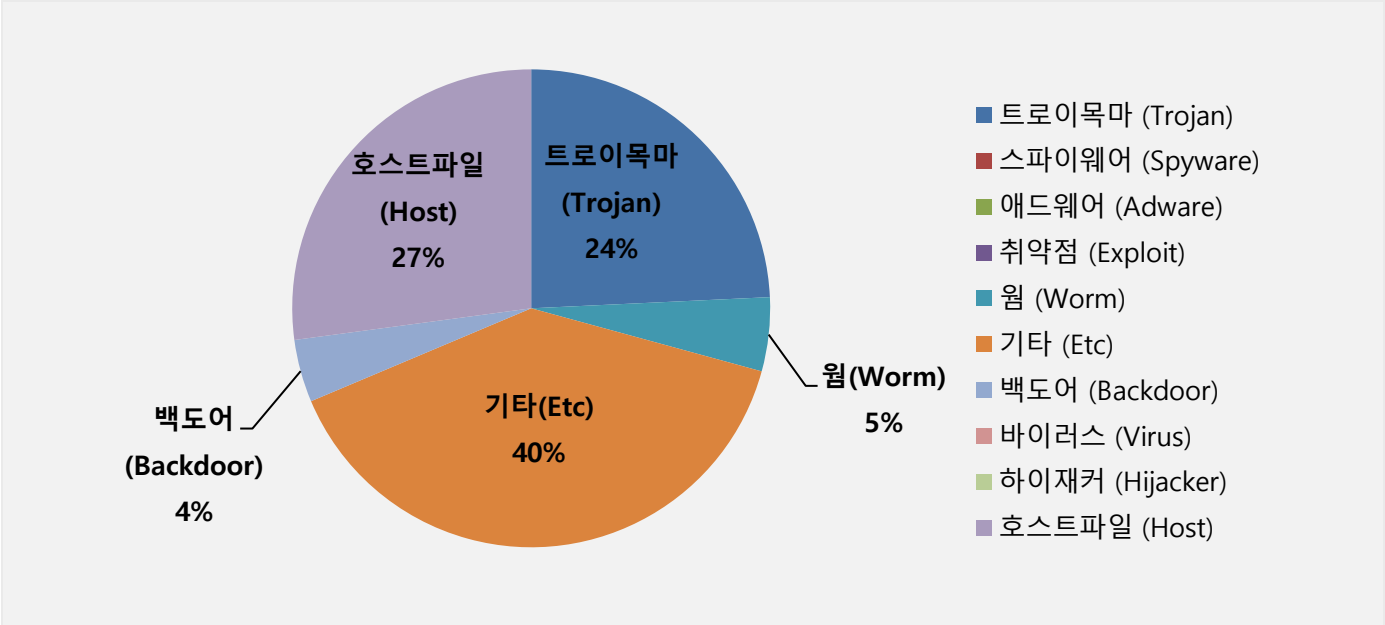
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 1	Hosts.media.opencandy.com	Host	724,350
2	↑ 1	Misc.HackTool.AutoKMS	ETC	426,553
3	↑ 1	Trojan.ShadowBrokers.A	Trojan	243,388
4	↑ 2	Misc.HackTool.KMSActivator	ETC	210,818
5	↑ 4	Trojan.HTML.Ramnit.A	Trojan	156,163
6	↑ 5	Misc.Keygen	ETC	137,545
7	New	Gen:Variant.Johnnie.248927	ETC	133,964
8	↑ 6	Backdoor.Generic.792814	Backdoor	113,244
9	New	Generic.Brontok.8CAE5D8F	Trojan	105,791
10	↑ 3	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	91,432
11	↓ 1	Misc.Riskware.TunMirror	ETC	88,620
12	New	Worm.ACAD.Bursted	Worm	70,803
13	New	Worm.ACAD.Bursted.doc.B	Worm	62,657
14	New	Gen:Variant.Ursu.489129	ETC	54,769
15	New	Trojan.Agent.EZVL	Trojan	51,165

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 12 월 01 일 ~ 2020 년 12 월 31 일

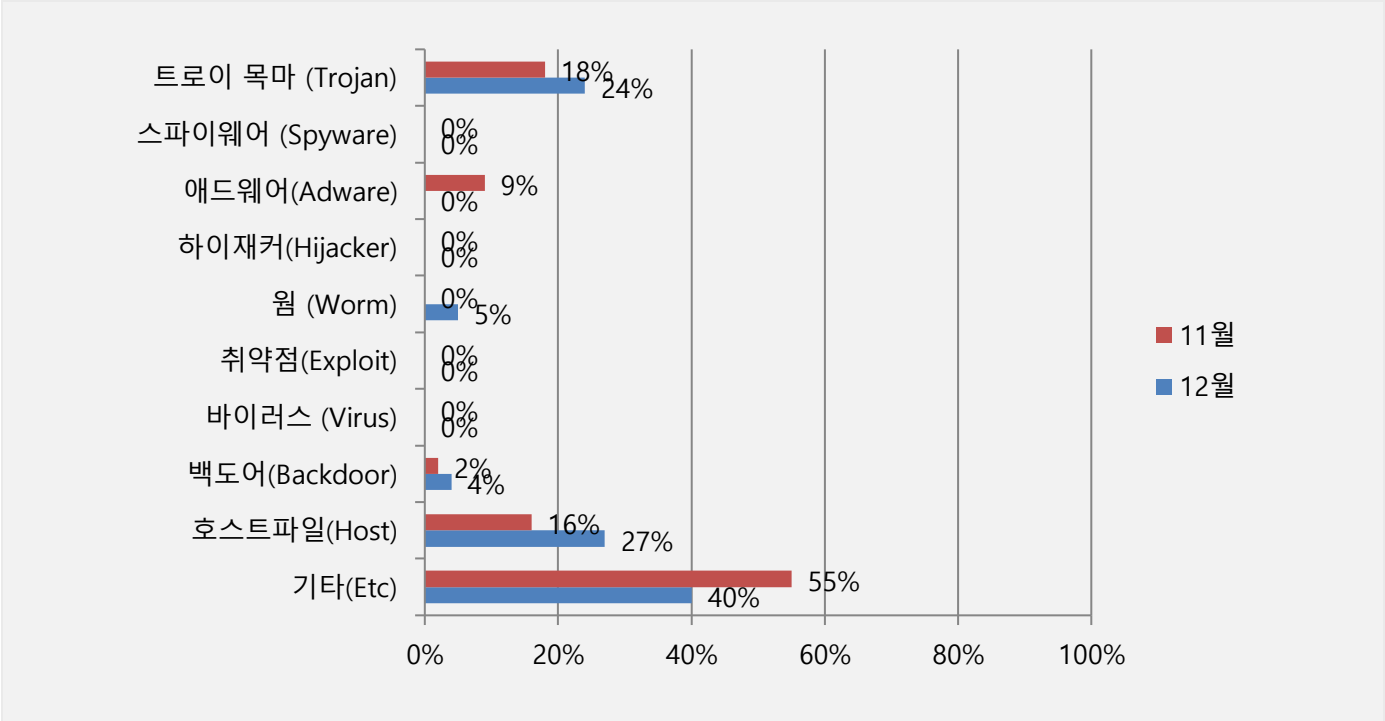
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 40%를 차지했으며 트로이목마(Trojan) 유형이 24%로 그 뒤를 이었다. 지난달 미미한 수치를 보이던 웜(Adware) 유형의 비율이 5%로 소폭 상승했으며 11 월과 비교하여 전체 감염 건수는 약 39% 감소하였다.



카테고리별 악성코드 비율 전월 비교

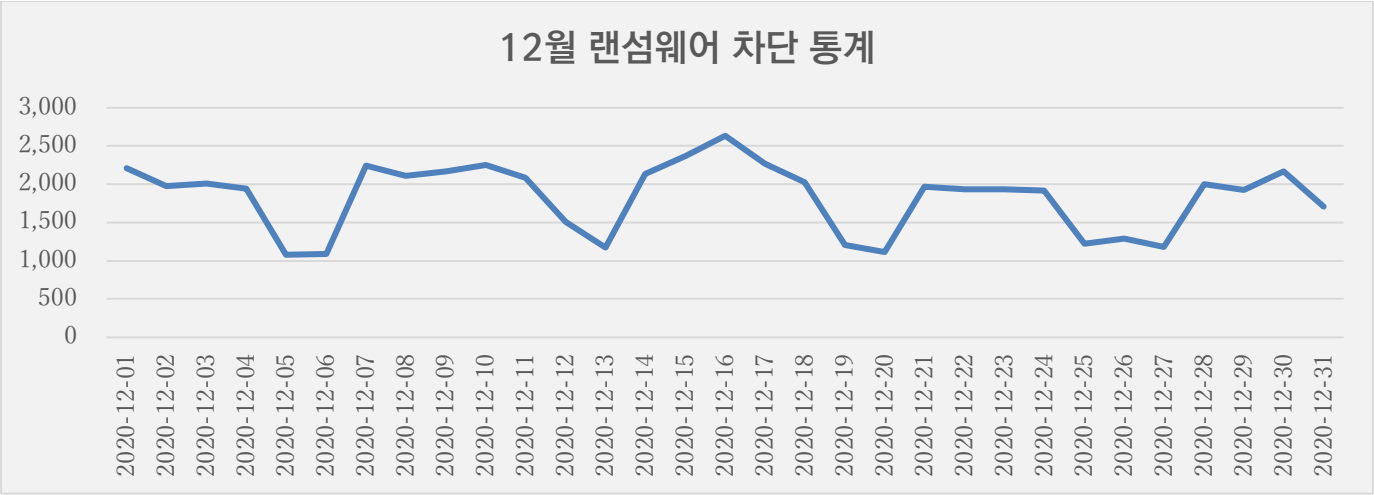
12 월에는 11 월과 비교하여 트로이목마(Trojan) 유형과 호스트파일(Host) 유형의 악성코드 감염 비율이 각각 6%, 11% 증가하였다. 또한 지난달에는 큰 비중을 차지하지 않던 웜(Worm) 악성코드의 감염 비율이 5%로 증가하였다. 지난 11 월에 다수 탐지됐던 애드웨어(Adware) 악성코드 유형은 이번 달에는 급감하여 악성코드 탐지율 Top15 내에 기록되지 못했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

12 월 랜섬웨어 차단 통계

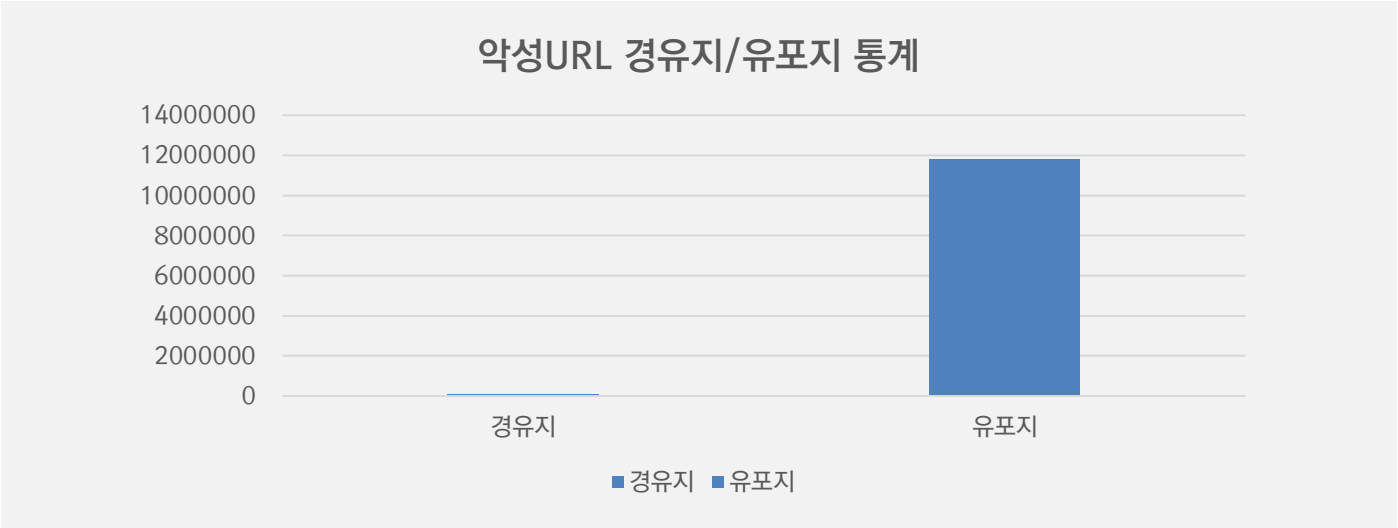
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 12 월 1 일부터 12 월 31 일까지 총 56,874 건의 랜섬웨어 공격 시도가 차단되었다. 11 월에 비해 랜섬웨어 공격 건수는 약 3.2% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 12 월 한 달간 총 11,861,707 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 11 월 한 달간 확인되었던 14,565,367 건의 악성코드 경유지/유포지 URL 수에 비해 약 18% 가량 감소한 수치다.

악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바란다.



02

전문가 보안 기고

1. 2020 년 4 분기, 알약 랜섬웨어 행위기반 차단 건수: 172,696 건!

2. 지속적으로 유포되는 '이미지 저작권 침해' 메일 주의

1. 2020 년 4 분기, 알약 랜섬웨어 행위기반 차단 건수: 172,696 건!

2020 년 4 분기, 알약을 통해 총 172,696 건의 랜섬웨어 행위기반 공격이 차단된 것으로 확인되었습니다.

이번 통계는 개인 사용자를 대상으로 무료 제공하는 공개용 알약의 '랜섬웨어 행위 기반 차단 기능'을 통해 차단된 공격만을 집계한 결과로, 패턴 기반 탐지건까지 포함한다면 전체 공격은 더욱 많을 것으로 예상됩니다.

통계에 따르면, 2020 년 4 분기 알약을 통해 차단된 랜섬웨어 공격은 총 172,696 건으로, 이를 일간 기준으로 환산하면 일 평균 약 1,910 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다. 다만, 2018 년부터 현재까지 약 2 년에 걸쳐 전체 랜섬웨어 공격 건수는 지속적으로 감소되고 있는 추세를 보이고 있습니다.

[그림] 알약 랜섬웨어 행위기반 차단 기능'을 통해 차단된 2020 년 4 분기 랜섬웨어 공격 통계

ESRC 는 2020 년 4 분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

1) 국내 유명 유통 대기업을 대상으로 하는 Clop 랜섬웨어 캠페인으로 큰 피해 발생
2) '비너스락커' 그룹이 유포하는 RaaS 형태의 Makop 랜섬웨어 공격 꾸준히 발생
3) LockBit, MalLocker, RansomEXX 등 새로운 버전을 사용한 랜섬웨어 공격 다수 발생

02 전문가 기고

2020 년 4 분기에는 다양한 사회적 이슈를 활용하여 사용자로 하여금 랜섬웨어 이메일 첨부파일을 열어보도록 유도하는 Clop, Sodinokibi, Makop 랜섬웨어가 꾸준히 상위권을 유지했으며, 랜섬웨어 공격 건수는 10 월과 11 월에 다소 증가하였다가 12 월에는 감소 추세를 나타냈습니다.

4 분기에는 주목할만한 위협으로는 11 월에 발생한 Clop 랜섬웨어의 국내 유통 대기업을 타깃으로 하는 공격으로 해당 기업은 상당한 금전적 피해를 입었습니다. Clop 랜섬웨어 해커들은 사전에 기업 내부 시스템을 조사하여 맞춤형 악성 파일을 사용해 공격을 수행하는 치밀함을 보였으며, 확장명을 변경하는 이전 변종들과 달리 원본 파일명을 그대로 사용함으로써 피해자들의 의심을 피할 수 있었습니다.

10 월에는 Sodinokibi 랜섬웨어 해커들이 파일리스 기반의 새로운 변종을 사용하여 공격을 수행한 것으로 확인되었습니다. 악성코드는 주로 피싱 페이지에서의 다운로드를 통해 유포되며, 취약한 Wordpress 환경에서 악성 게시글을 포스팅하여 사용자를 유인하는 방식을 사용했습니다. 12 월에는 Gootkit 정보 탈취 트로이 목마가 독일을 타깃으로 하는 새로운 캠페인에서 Sodinokibi 랜섬웨어를 유포한 정황도 확인되었습니다.

또한 비너스락커 그룹이 10 월부터 12 월까지 Makop 랜섬웨어를 꾸준히 유포한 것으로 확인되었습니다. 주로 이력서, 저작권 위반, 부당 전자상거래 위반 등의 테마를 활용한 스피어피싱 공격을 수행하였습니다.

이밖에도 LockBit, MalLocker, RansomExx 등 기존의 방식에 새로운 기능을 추가하여 공격을 수행한 여러 랜섬웨어가 확인되었습니다. 은밀하게 내부 네트워크 이동을 통해 감염을 시도하는 LockBit 랜섬웨어, 이전 버전에서는 활용한 적 없는 안드로이드 홈 버튼을 통해 랜섬노트를 표시하고, 오픈소스 기계 학습 모듈을 사용해 오버레이 화면을 기기 화면 크기에 자동으로 맞추는 기능을 탑재하여 등장한 MalLocker 랜섬웨어, 리눅스 버전을 개발해 운영을 확대하고 있는 RansomExx 랜섬웨어 등이 대표적입니다.

ESRC 센터장 문종현 이사는 “2020 년 4 분기 내 유포된 랜섬웨어 중 비너스락커 조직이 Makop 랜섬웨어를 지속 활용한 정황이 수십 차례 포착된 바 있다."고 언급하며, "ESRC 에서 선정한 주요 동향 외에도 해외 기업과 산업 시스템을 주로 노렸던 대규모의 랜섬웨어 캠페인의 경우 국내에서는 아직 피해사례가 확인되지 않았으나 미리 대비하는 자세가 필요하다."고 강조했습니다.

이밖에 ESRC 에서 밝힌 2020 년 4 분기에 새로 발견되었거나, 주목할 만한 랜섬웨어는 다음과 같습니다.

02 전문가 기고

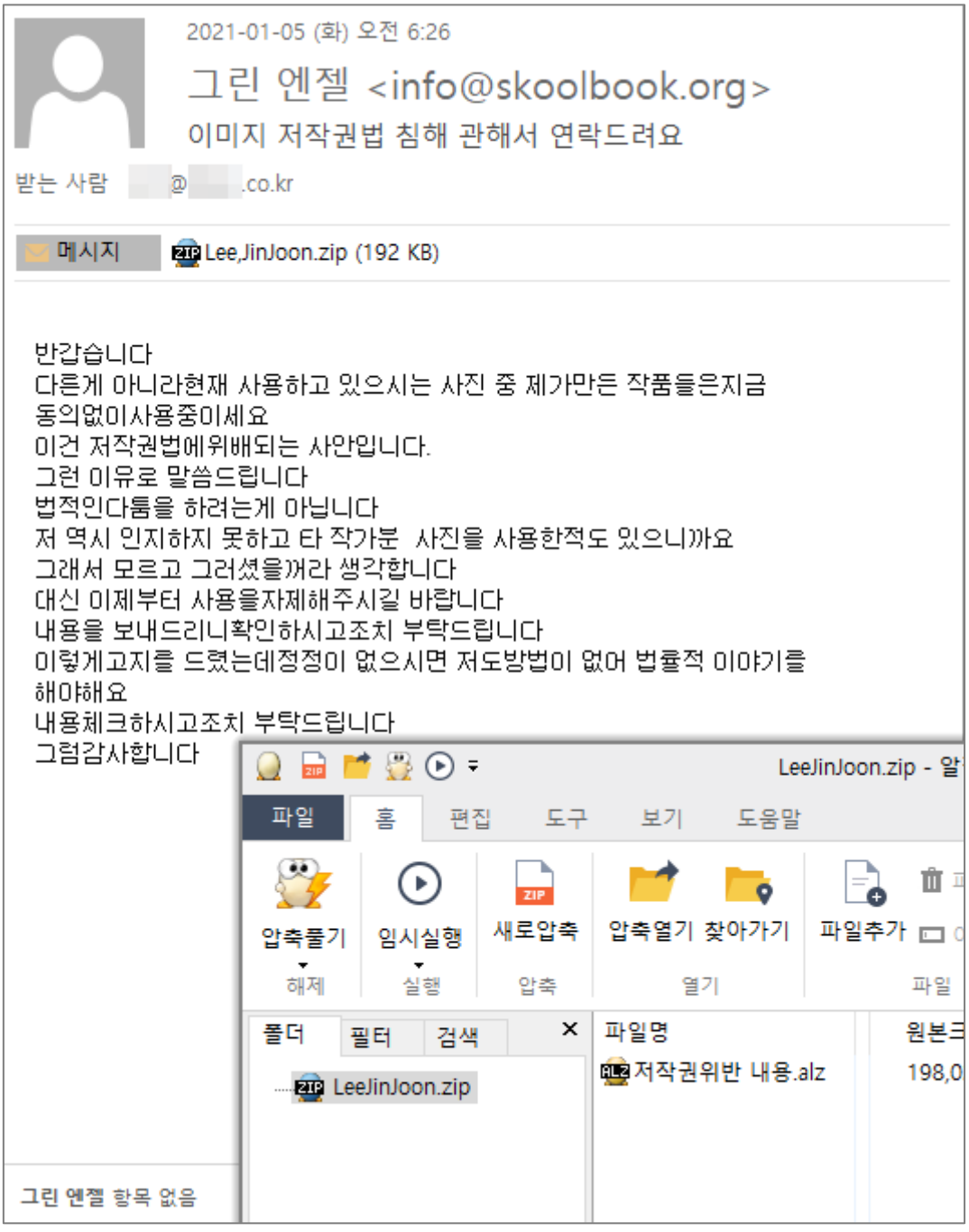
랜섬웨어 명	주요 내용
Clop	주로 기업을 대상으로 공격을 수행하는 랜섬웨어로 기업 내부 시스템을 사전에 조사하여 맞춤형 악성파일을 사용함으로써 사전 차단이 어려운 것이 특징. 또한 기존 변종들은 암호화된 파일 확장명을 변경하는 방식으로 진행되었지만, 최근 공격에서는 원본 파일명을 그대로 유지함.
Myransom	PDF 가 아닌 PDX 파일 아이콘을 사용하는 랜섬웨어로 일반적인 랜섬웨어와 다르게 확장자 변경이 이루어지지 않는 점이 특징. White 랜섬웨어로도 알려져있으며 최근 국토교통부를 사칭해 청년 인턴 관련 내용으로 파일 실행을 유도함으로써 감염을 시도함.
CoderWare	유명 콘솔게임 'Cyberpunk 2077'으로 위장한 윈도우/모바일 랜섬웨어로 BlackKingdom 랜섬웨어의 변종으로 확인됨. 불법 복제 버전 소프트웨어로 위장해 게임 인스톨러, 치트엔진, 크랙 등의 이름으로 유포됨.
RegretLocker	가상 하드 드라이브(VHD)를 암호화하는 랜섬웨어로 암호화 시작 전 디스크 검사를 통해 가상 하드 디스크 파일을 찾아 오프라인이거나 분리되어 있는 경우 재연결하여 내부 파일 암호화 진행하는 것이 특징.
Fonix	비교적 새로운 형태의 서비스형 랜섬웨어로 다양한 사이버 범죄 포럼에서 여러 제품 형태로 판매됨. 기존의 RaaS 와 달리 4 가지 암호화 방법을 조합하여 사용하기 때문에 암호화 속도가 느리며, 감염 후 사이클이 복잡하여 운영이 쉽지 않은 것이 특징.
Ranzy Locker	Windows 가상 머신을 대상으로 공격을 수행하는 ThunderX 랜섬웨어 변종. 이전 버전 복호화툴이 공개된 후 새롭게 유포되었으며, 주요 특징들은 이전과 유사함. 많은 랜섬웨어 공격 방식과 유사하게, 데이터 유출을 빌미로 협박하는 이중 탈취 기법을 사용함.
Nefilim	유효한 디지털서명이 포함된 기업 표적형 랜섬웨어로 기업 네트워크에 침투하여 정보를 외부로 유출한 후 마지막 단계에서 파일 암호화 행위를 진행하는 것이 특징. 최근 미국 가전 회사를 대상으로 정보 유출 협상을 시도하였으나 실패함.
Sodinokibi	최근 파일리스 기반의 새로운 방식을 도입한 랜섬웨어로, BlueCrab 이라는 이름으로도 알려짐. 취약한 Wordpress 환경의 웹 서버를 탈취한 후, 악성 게시글을 통해 다운로드 페이지로 위장한 피싱 페이지를 유포함.
Makop	주로 비너스락커 조직이 유포하는 랜섬웨어로 최근 기존의 파일 기반에서 레지스트리 방식의 파일리스 기반으로 변화한 것이 특징. 이를 통해 윈도우 부팅시마다 자동 재실행되도록 함으로써 공격 성공률을 높임.

랜섬웨어 유포 케이스의 대다수는 이메일 형태지만, 코로나 19 바이러스 확산 방지를 위해 재택 근무를 수행하는 임직원이 증가함에 따라 기업 내부망 접속을 위해 사용되는 재택 근무 단말기 OS/SW 보안 업데이트 점검을 의무화하고 임직원 보안 인식 교육도 병행해야 합니다.

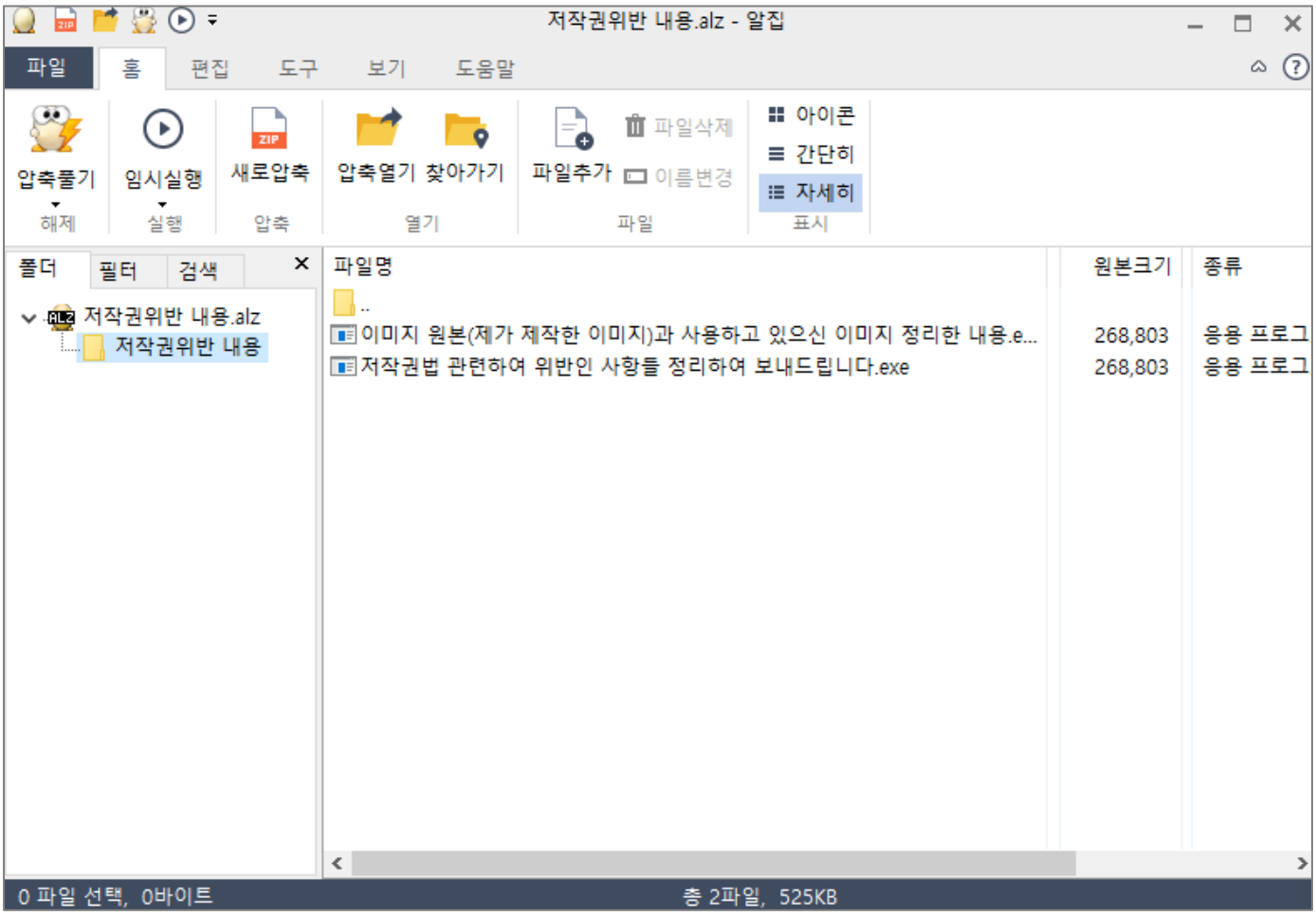
이스트시큐리티는 랜섬웨어 감염으로 인한 국내 사용자 피해를 미연에 방지하기 위해, 한국인터넷진흥원(KISA)과의 긴밀한 협력을 통해 랜섬웨어 정보 수집과 유기적인 대응 협력을 진행하고 있습니다.

2. 지속적으로 유포되는 '이미지 저작권 침해' 메일 주의

이미지 저작권법 위배 안내로 위장한 메일을 통해 Makop 랜섬웨어가 지속적으로 유포되는 정황이 포착되어 일반 사용자와 기업 담당자들의 주의가 필요합니다.



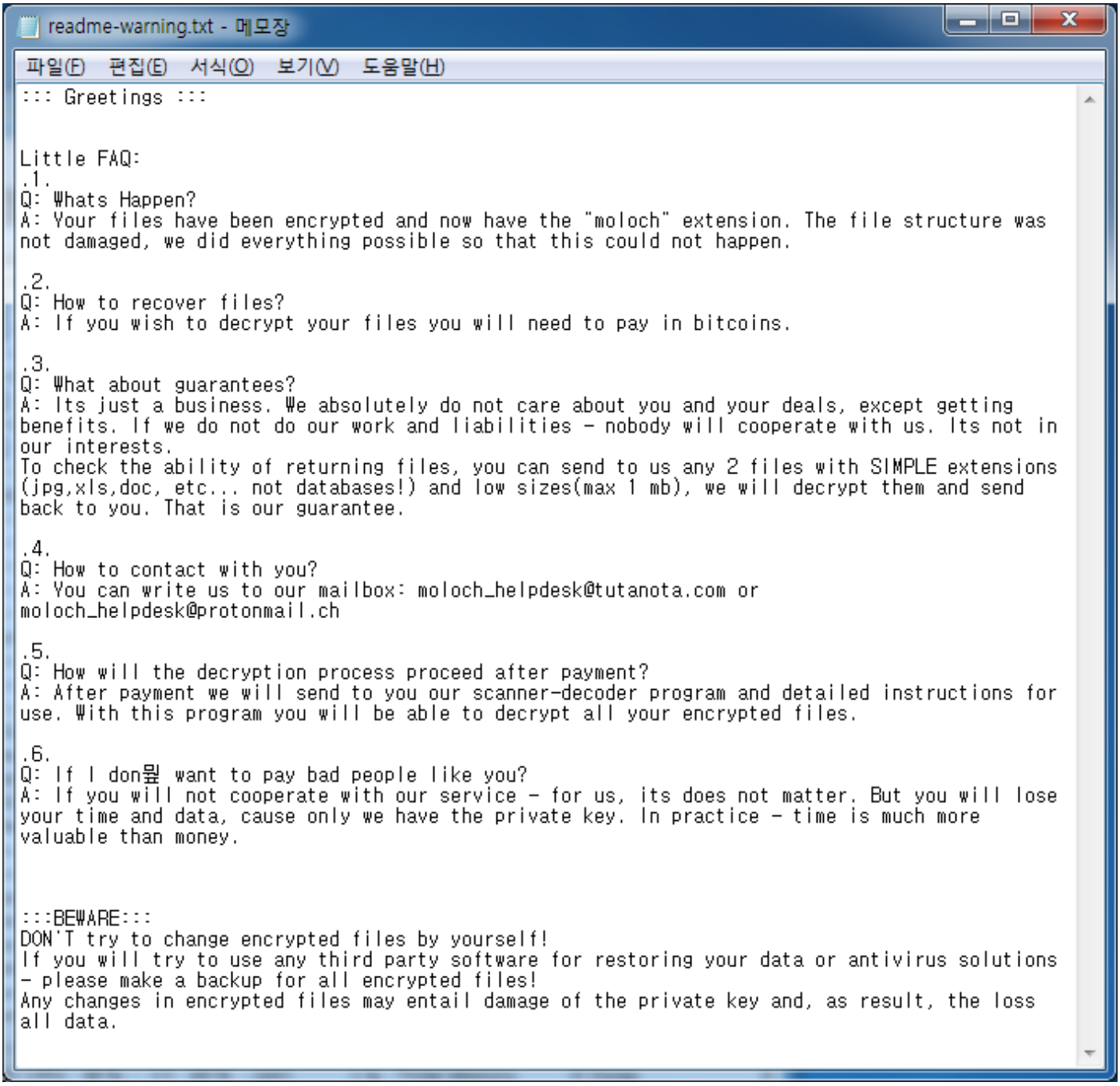
[그림 1] 이미지 저작권법 침해 관련 악성 메일



[그림 2] 저작권위반 내용.alz 파일 내용

만일 이용자가 최종 압축 파일에 있는 '이미지 원본(제가 제작한 이미지)과 사용하고 있으신 이미지 정리한 내용.exe', '저작권법 관련하여 위반인 사항들 정리하여 보내드립니다.exe'을 클릭할 경우 파일 암호화 기능의 Makop 랜섬웨어가 실행됩니다.

Makop 랜섬웨어는 파일 암호화 기능을 수행하는 악성코드로 암호화된 파일 뒤에 [임의 영문 8자리].[moloch_helpdesk@tutanota.com].moloch 를 추가하고, 이후 복호화 안내를 위해 'readme-warning.txt'를 드롭합니다. 아래는 makop 랜섬웨어의 랜섬노트로 'moloch_helpdesk@tutanota.com', 'moloch_helpdesk@protonmail.ch' 메일로 연락해달라는 내용을 담고 있습니다.



[그림 3] 랜섬노트(readme-warning.txt) 파일 화면

관련하여 2020 년 12 월 중순부터 금일 확인된 메일과 유사한 형태로 보내진 정보입니다. 특징적으로 송신자 이름을 (색상) + (엔젤, 드론, 망고 등)의 형태로 조합한 점, 첨부 파일 이름은 한국식 이름으로 되어있습니다. 이를 통해 지속적으로 비너스락커 조직이 국내를 대상으로 하고 있음을 알 수 있습니다.

송신자 이메일	송신자 이름	첨부파일 이름
info@skoolbook.org	그린엔젤	Lee,JinJoon.zip
marek.pokorny@hcjicin.cz	블랙드론	Gil,MinJoon.alz
e****@********.co.kr	옐로우망고	Gil,SungWoong.alz
e****@********.co.kr	브라운핀	Kim,MinSang.alz
mauro.cassano@alphacaesar.it	옐로우마린	Kim,MinSang.alz
c.franco@cnjap.pt	화이트엔젤	Gil,MinJoon.alz
c.franco@cnjap.pt	그린망고	Oh,HanDong.alz
kompo@kompoarredamenti.it	블루망고	Gil,MinJoon.alz
contact@ga-immobilier.com	블루핀	Gil,SungWoong.alz

[표 1] 2020 년 12 월 중순부터 보내진 유사 메일 종류

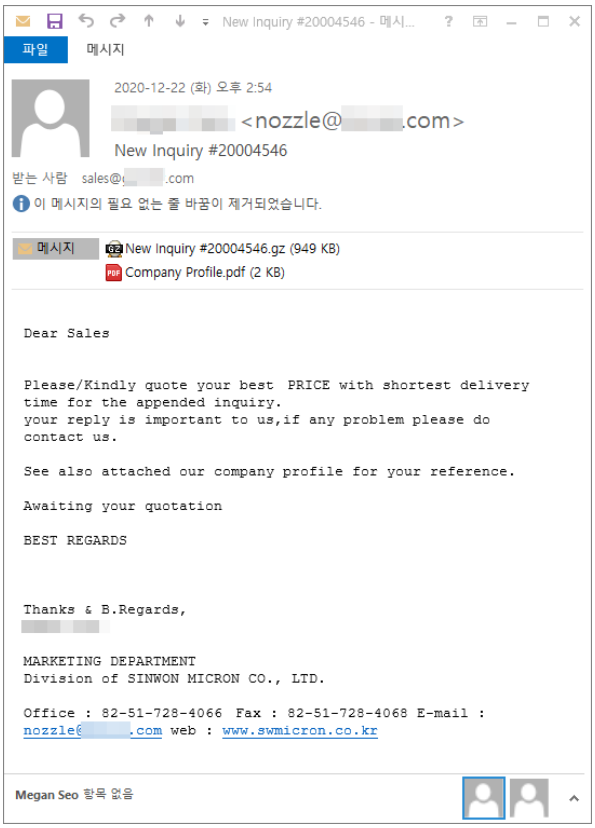
따라서 저작권이라는 민감한 소재로 사용자들에게 첨부파일을 실행시키도록 유도하기 때문에 불분명한 파일 실행을 하지 않는 등의 사용자들의 각별한 주의가 필요합니다. 또한 중요한 파일들은 정기적으로 외장 매체(USB, 외장 HDD) 등에 백업해두는 습관이 필요합니다.

현재 알약에서는 'Trojan.Ransom.Makop'으로 진단하고 있습니다.

03
악성코드 분석 보고

[Spyware.AgentTesla] 악성코드 분석 보고서

최근 'Spyware.AgentTesla'(이하 'AgentTesla') 악성코드가 국내 기업을 대상으로 무역 관련 내용의 악성 메일로 유포되고 있다. 메일 첨부 파일에 있는 'New Inquiry #20004546.gz' 내 'New Inquiry #20004546.exe'에서 실행이 이루어진다.



[그림 1] 무역 관련 내용으로 위장한 악성 메일

실행되는 'AgentTesla'는 SMTP를 통해 C&C로 감염 PC의 정보를 전송하는 악성코드이다. 따라서 감염될 경우 사용자들이 사용하는 크리덴셜 정보들이 공격자에게 노출될 수 있어 주의가 필요하다.

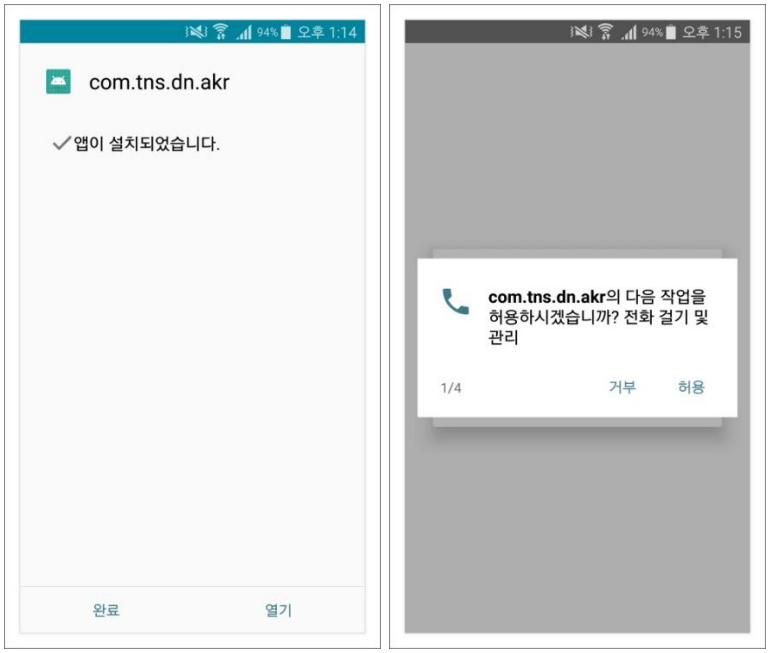
또한 기업 혹은 최근 재택근무 환경에서 감염이 되는 경우, 크리덴셜 정보의 유출에 따른 피해가 발생할 수 있어 주의가 필요하다.

현재 알약에서는 'Spyware.AgentTesla'로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.AgentNK] 악성코드 분석 보고서

북한의 사이버 공격이 지속적으로 이어지고 있다. PC 환경은 물론 모바일 기기를 향한 공격 빈도도 증가하고 있다. 김수키(Kimsuky)로도 알려진 탈륨(Thallium) 그룹이 유포한 "Trojan.Android.AgentNK"는 피해자의 개인 정보 탈취를 목적으로 하고 있다.

개인의 일상과 밀접하게 연결된 모바일 기기의 특성상 개인 정보가 많을 수밖에 없으며 공격자들은 이점을 노리고 모바일 기기 대상의 악성 앱을 유포하는 것이다.



[그림] 설치 시 화면

분석 내용을 살펴보면 Trojan.Android.AgentNK 는 피해자의 개인 정보 탈취를 주요 목적으로 하고 있음을 알 수 있다. 그리고 탈취한 개인 정보들을 바탕으로 추가 공격을 감행할 것으로 판단된다.

이런 공격은 사용자의 예방 노력이 무엇보다 중요하다. 앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약 M 과 같은 신뢰할 수 있는 백신을 사용하여야 하겠다.

현재 알약 M 에서는 해당 앱을 'Trojan.Android.AgentNK' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

Gootkit 악성코드, Sodinokibi 랜섬웨어와 함께 부활해

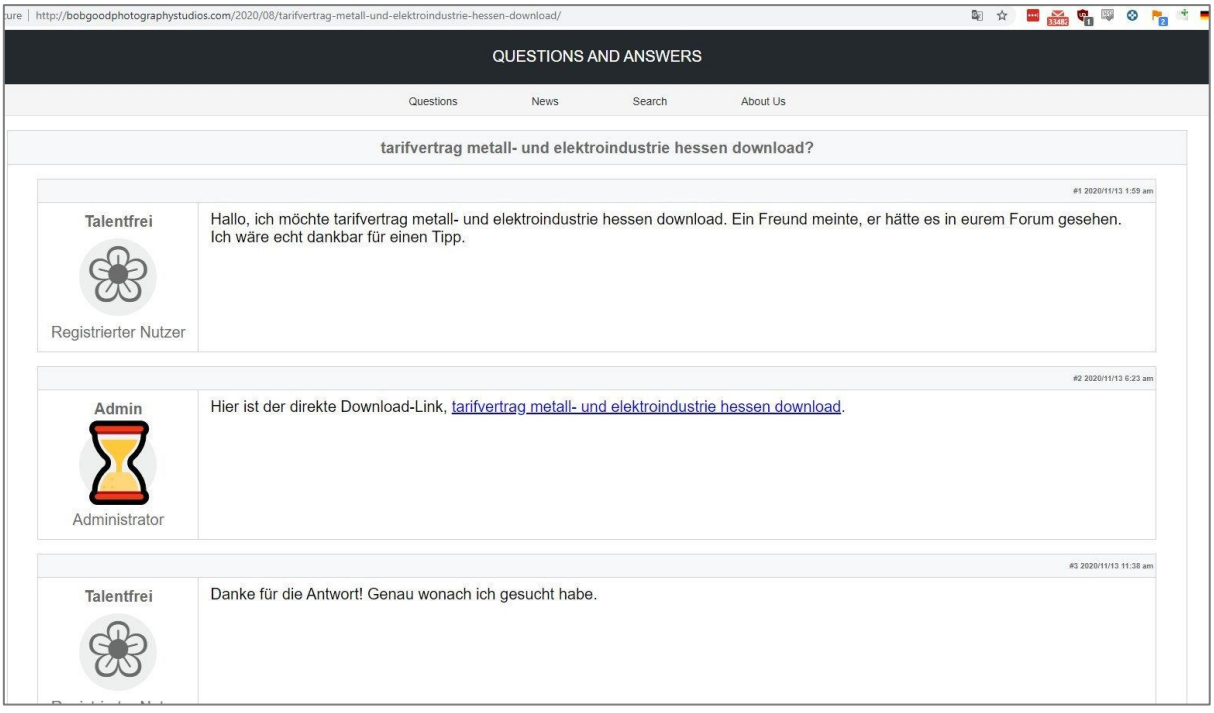
Gootkit malware returns to life alongside REvil ransomware

1 년 간의 공백 끝에, Gootkit 정보 탈취 트로이목마가 독일을 노리는 새로운 캠페인과 함께 부활했다. Gootkit 트로이목마는 자바스크립트 기반 악성코드로 공격자에게 원격 접속 제공, 키 로깅, 영상 녹화, 이메일 탈취, 비밀번호 탈취, 온라인 은행 자격 증명을 훔치기 위해 악성 스크립트를 주입하는 등 다양한 악성 행위를 수행한다.

2019 년, Gootkit 공격자들은 인터넷에 MongoDB 데이터베이스를 노출해 정보 유출 사고를 겪었다. 이 사건 이후 GootKit 공격자들은 이번 달 다시 공격을 시작하기 전까지 활동을 중단한 것으로 알려져 있다.

GootKit, 랜섬웨어와의 파트너십 통해 부활

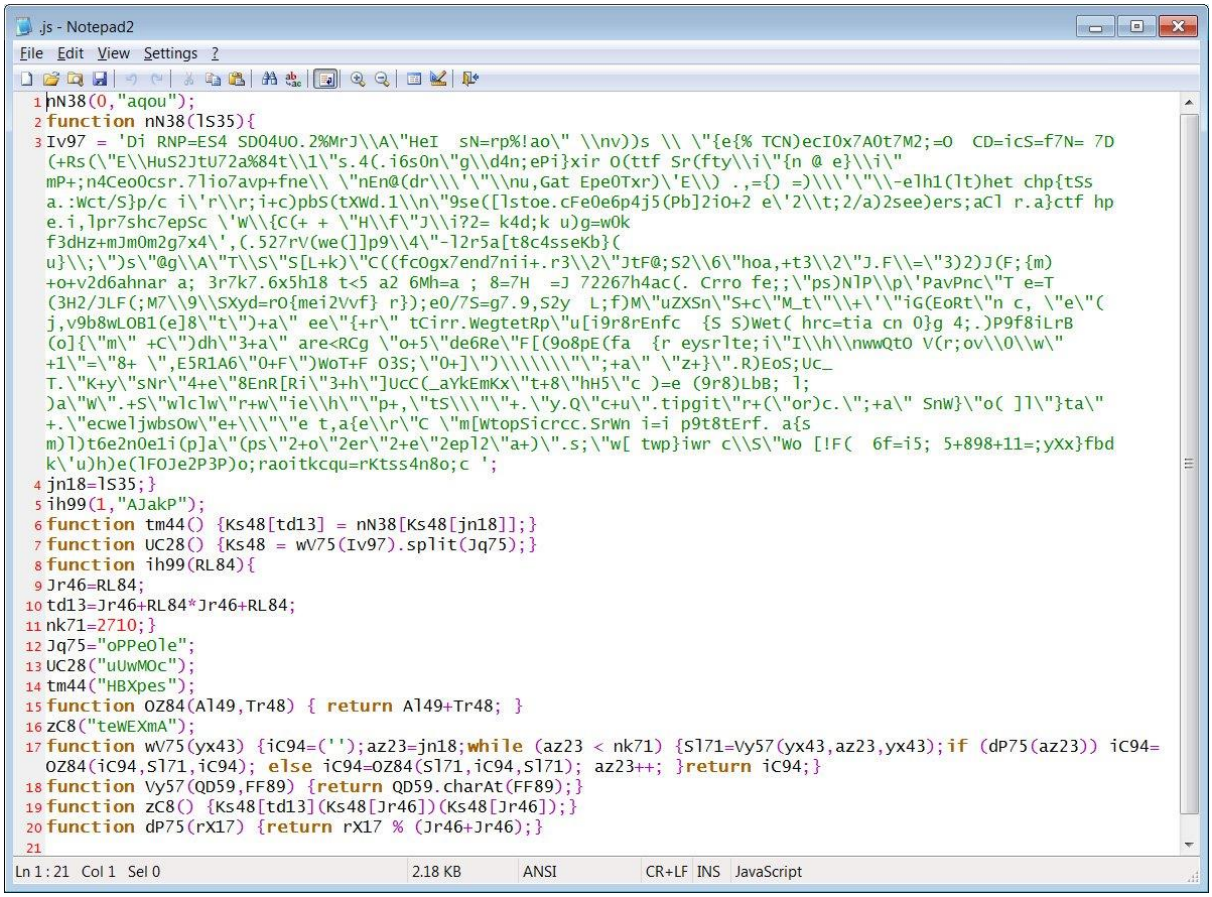
The Analyst 로 알려진 한 보안 연구원은 BleepingComputer 에 독일을 노린 공격에서 Gootkit 악성코드가 다시 발견되었다고 제보했다. 공격자는 이 새로운 악성 캠페인을 통해 워드프레스 사이트를 해킹하고 SEO 포이즈닝을 통해 방문자에게 가짜 포럼 게시물을 표시한다. 이 가짜 게시물은 가짜 양식 또는 다운로드로 연결되는 링크를 포함한 질답으로 위장한다.



[그림] Gootkit 캠페인에서 발견된 가짜 포럼 게시물

[이미지 출처] https://www.bleepingcomputer.com/news/security/gootkit-malware-returns-to-life-alongside-revil-ransomware/

사용자가 링크를 클릭하면, Gootkit 악성코드나 Sodinokibi 랜섬웨어를 설치하는 난독화된 JS 파일이 포함된 ZIP 파일을 다운로드하게 된다.



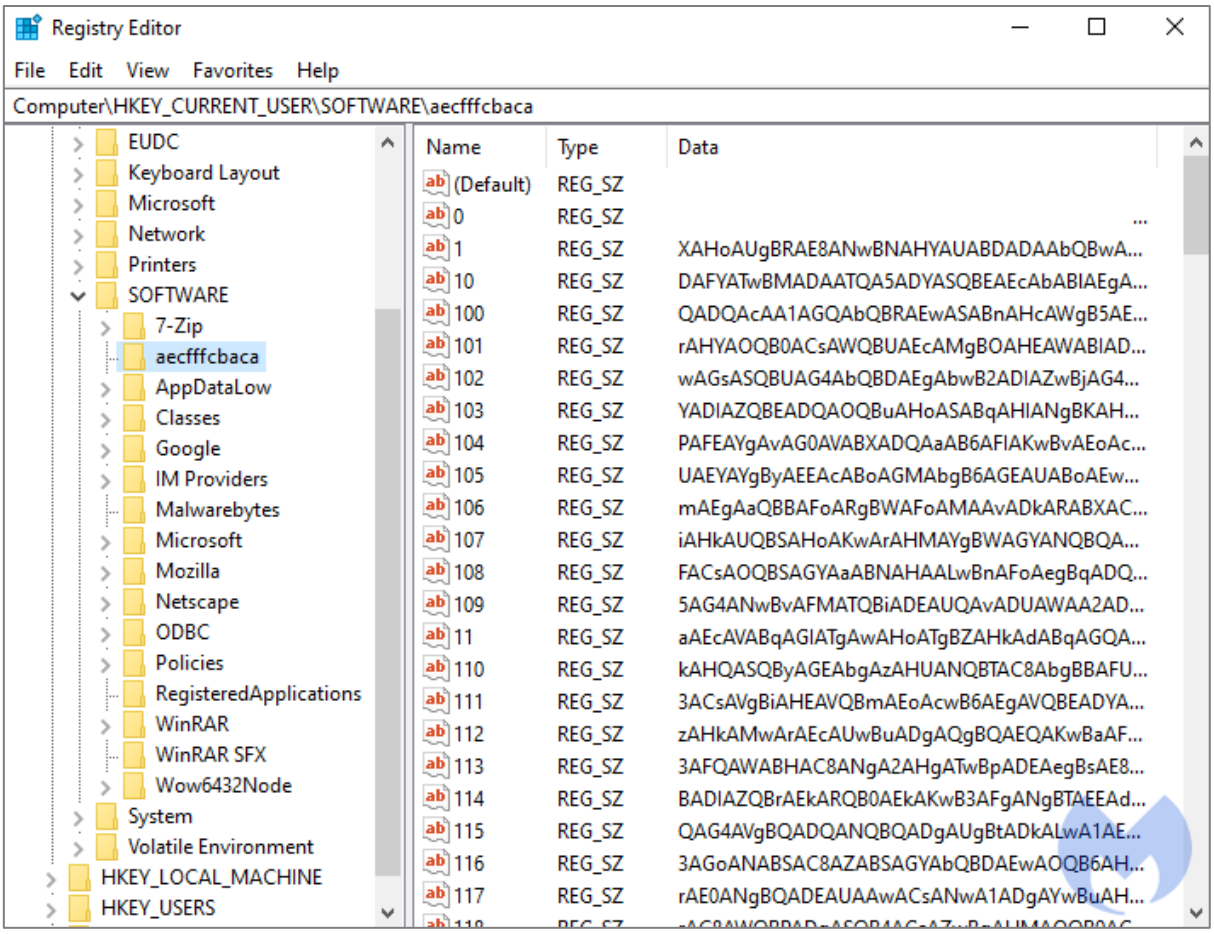
[그림] 난독화된 JS 스크립트

[이미지 출처] https://www.bleepingcomputer.com/news/security/gootkit-malware-returns-to-life-alongside-revil-ransomware/

이 방법과 동일한 배포 방식은 Gootkit 이 활동을 중단했던 시기인 2019 년 9 월 Sodinokibi 가 사용했다.

Gootkit 과 Sodinokibi, 파일리스 공격 통해 설치돼

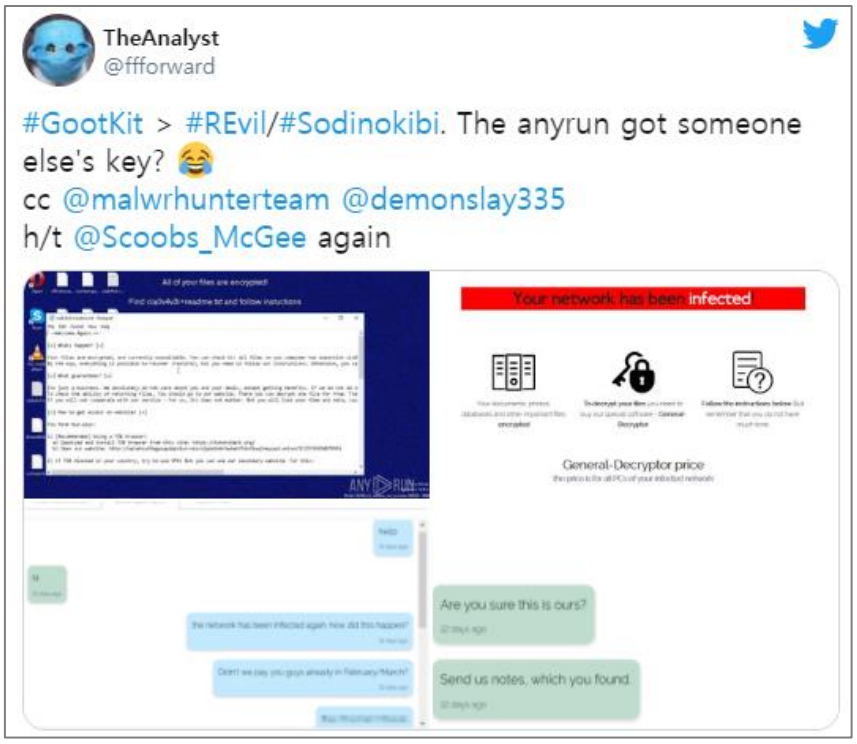
Malwarebyte 의 연구원들은 보고서를 통해 해당 악성 JavaScript 페이로드가 파일리스 Gootkit 또는 Sodinokibi 공격을 실행할 것이라 설명했다. 이 JavaScript 가 실행되면, 명령 및 제어 서버에 연결해 악성코드 페이로드를 포함한 또 다른 스크립트를 다운로드한다. Malwarebytes 의 분석에 따르면, 이 페이로드는 보통 Gootkit 이지만 일부 경우 Sodinokibi 랜섬웨어가 나오기도 한다. 이 페이로드는 base64 로 암호화되었거나, 텍스트 파일에 16 진수 문자열 형태로 저장되어 있거나 아래와 같이 수많은 윈도우 레지스트리 값으로 분할된다.

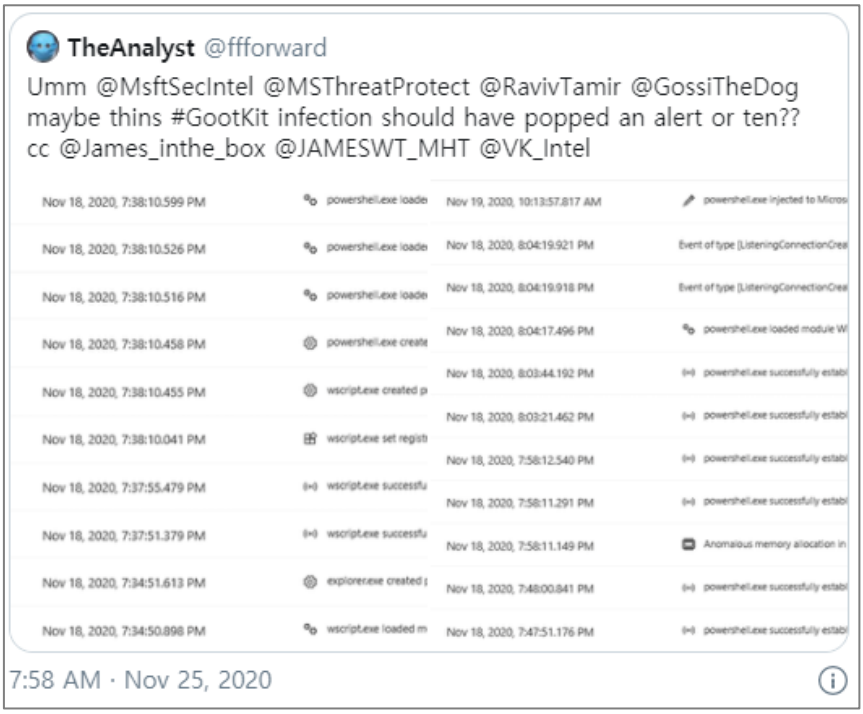


[그림] 윈도우 레지스트리에 저장된 페이로드

[이미지 출처] https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

이 로더는 결국 레지스트리 또는 텍스트 파일의 페이로드를 읽고 디코딩한 다음 파일 없이 메모리에서 직접 프로세스를 시작한다. 난독화된 페이로드를 사용하고 레지스트리에 조각으로 분리해 저장할 경우 보안 소프트웨어가 악성 페이로드를 탐지하기 어려워진다. The Analyst 는 이 악성 캠페인을 테스트하던 중 흥미로운 사실을 발견했다. 바로 Sodinikibi 가 이전 공격에 사용된 랜섬 노트를 드롭한다는 것이다.





[이미지 출처] https://twitter.com/ffforward/status/1331371583890485257

이 오류는 공격자들이 캠페인을 배포할 때 Sodinokibi 랜섬웨어를 새 버전으로 교체하는 것을 잊어버렸기 때문에 발생한 것으로 추측된다.

[출처] https://www.bleepingcomputer.com/news/security/gootkit-malware-returns-to-life-alongside-revil-ransomware/
https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

범죄자들, '블랙박스 공격' 통해 이탈리아 ATM 에서 80 만 유로 훔쳐

Crooks stole 800,000€ from ATMs in Italy with Black Box attack

한 범죄조직이 새로운 블랙박스(Black Box) 공격 기법을 사용하여 이탈리아 은행에서 운영하는 ATM 과 우체국 현금 지급기 최소 35 곳에서 돈을 훔친 것으로 나타났다. 이탈리아의 법 집행 기관은 해당 사이버 범죄 조직이 ATM 블랙박스 공격을 통해 약 7 개월 만에 약 80 만 유로(한화 약 10 억 6 천만 원)를 훔쳤다고 밝혔다.

[이미지 출처]https://twitter.com/Bank_Security/status/1332335834234818561

이탈리아 경찰은 이 사건과 관련된 12 명을 확인했으며, 중 6 명은 이미 체포했고 3 명은 폴란드에서 제한된 상태이며 1 명은 몰도바로 돌아왔으며 2 명은 이탈리아 영토에 있지 않을 것이라 추측된다고 밝혔다. 현지 언론에 따르면, 이 범죄 그룹은 밀라노, 몬차, 볼로냐, 모데나, 로마, 비테르보, 만투아, 비첸차, 파르마 지방에 수 많은 물류 기지를 소유하고 있었던 것으로 나타났다.

블랙박스 공격은 "블랙박스" 기기를 통해 ATM 기계가 현금을 내놓도록 하는 명령어를 보내는 일종의

잭포팅(jackpotting) 공격이다. 이 공격을 실행하기 위해서는 모바일 기기나 라즈베리와 같은 블랙박스 기기가 ATM 에 물리적으로 연결되어야 한다. 공격자는 이를 이용하여 기기에 명령을 보낼 수 있다. ATM 블랙박스 공격은 언더그라운드에서 꽤 인기있는 공격 방식이며, 여러 공격자들은 ATM 기기를 해킹할 수 있는 하드웨어 장비와 악성코드를 제공하고 있다. 해킹된 ATM 기기 목록은 다음과 같다.

- UFF PP TT 12/07/2020 BELLUSCO
- BANCA POPOLARE DI NOVARA 07/16/2020 CRODO
- BPM 07/18/2020 WEEKLY
- BPM 07/20/2020 MORAZZONE
- UFF PP TT 03/08/2020 SANT'ILARIO D'ENZA
- CASSA SAVINGS 04/08/2020 SAONARA
- UFF PP TT 08/05/2020 CARUGATE
- UFF PP TT 08/08/2020 PESSANO WITH BORNAGO
- UFF PP TT 08/18/2020 SEVESO
- UFF PP TT 08/19/2020 FAGNANO OLONA
- BBPM 08/21/2020 COMO
- BANCA INTESA 08/27/2020 GRONTARDO
- BBPM 01/09/2020 BREMBATE DI ABOVE
- UFF PP TT 01/09/2020 SIZIANO
- UFF PP TT 02/09/2020 MELZO
- UFF PP TT 09/04/2020 CARATE BRIANZA
- UFF PP TT 07/09/2020 SENAGO
- UFF PP TT 11/09/2020 BRESCIA
- BPM 11/09/2020 PARMA
- UFF PP TT 09/14/2020 BUSNAGO
- BBPM 09/18/2020 ROZZANO
- BBPM 09/18/2020 CARONNO PERTUSELLA
- UFF PP TT 21/09/2020 GHEDI
- BBPM 09/22/2020 CASARILE
- BBPM 09/24/2020 MACHERIO
- BBPM 09/30/2020 RESCALDINA
- BBPM 09/30/2020 LIMENA
- VOLKS 21/10/2020 VILLAVERLA
- UNICREDIT 22/10/2020 GRISIGNANO DI ZOCCO

- BANCO S. MARCO 10/28/2020 SPINEA
- BANCA CAMBIANO 10/30/2020 MONTELUPO FIORENTINO
- BBPM 11/06/2020 BIASSONO
- BBPM 11/8/2020 Santo Srefano Ticino
- BCC 10/11/2020 Junction of Capannelle (RM)
- OFFICE PP. TT. 11/11/2020 Vermicino- Frascati

[이미지 출처] https://twitter.com/Bank_Security/status/1332335834234818561

공격자는 보안이 취약한 ATM 에서 모바일 기기를 연결하기 위해 케이스를 쉽게 조작할 수 있기 때문에 이러한 공격에 더욱 취약하다고 볼 수 있다. 지난 7 월, ATM 기계 제조 업체인 Diebold Nixdorf 는 모든 은행에 ATM 블랙박스의 새로운 변종, 잭포팅 공격에 대해 경고했다. 이 경고는 벨기에의 Agenta Bank 에서 잭포팅 공격을 받아 143 대 이상의 ATM 을 강제로 종료한 후 발행되었다. 해킹된 기기는 모두 Diebold Nixdorf ProCash 2050xe 장치였다. 벨기에 당국이 벨기에에서 이러한 범죄 행위를 발견한 것은 이번이 처음이다. Diebold Nixdorf 에서 발행한 경고에 따르면, 새로운 블랙박스 공격은 유럽 전역의 특정 국가에서 나타났다.

[출처] https://securityaffairs.co/wordpress/111659/cyber-crime/black-box-attack-italy.html
https://www.gazzettadiparma.it/italiamondo/2020/11/24/news/attacchi_informatici_da_800mila_euro_ai_bancomat_sgominata_banda_una_delle_basi_era_parma-4646532/

Gitpaste-12 봇넷, 리눅스 서버와 IoT 기기 노려

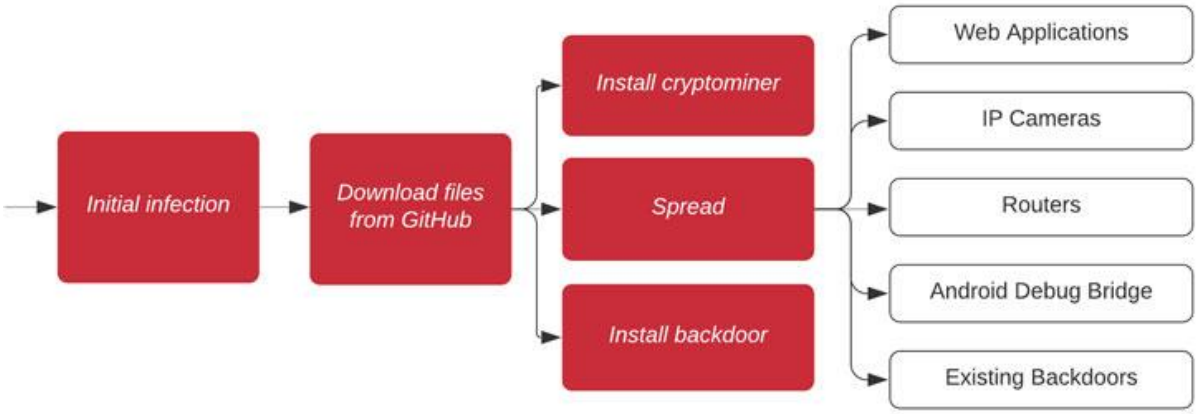
Wormable Gitpaste-12 Botnet Returns to Target Linux Servers, IoT Devices

타깃 시스템에 크립토마이너와 백도어를 설치하고 GitHub 과 Pastebin 을 통해 확산되는 새로운 웜 봇넷이 웹 애플리케이션, IP 카메라, 라우터를 해킹하기 위한 기능을 확장하여 돌아왔다. 11 월 초, Juniper Threat Labs 의 연구원들은 악성 코드를 호스팅하기 위해 GitHub 을 사용하는 "Gitpaste-12"라는 크립토마이너 캠페인을 발견했다. 이 악성코드는 Pastebin URL 에서 다운로드한 명령을 통해 실행되는 알려진 공격 모듈 12 개를 포함하고 있었다.

이 공격은 지난 10 월 15 일 시작해 10 월 30 일 Pastebin URL 과 저장소가 중단되기 전까지 12 일 동안 진행되었다. Jupiter 에 따르면, 11 월 10 일 두 번째 공격 웨이브는 다른 GitHub 저장소의 페이로드를 사용하여 시작되었다. 이 페이로드는 Linux 크립토마이너("ls"), 브루트포싱 공격을 위한 비밀번호 목록 파일 ("pass"), x86_64 리눅스 시스템에 대한 로컬 권한 상승 익스플로잇을 포함하고 있었다. 초기 감염은 Go 프로그래밍 언어로 작성된 바이너리인 X10-unix 를 통해 이루어진다. 이는 GitHub 에서 다음 단계 페이로드를 다운로드한다.

Juniper 의 연구원인 Asher Langton 은 지난 월요일 발표한 분석을 통해 아래와 같이 밝혔다.

"이 웜은 알려진 취약점 최소 31 개를 악용하여 웹 애플리케이션, IP 카메라, 라우터 등을 노리는 광범위한 공격을 수행한다. 이 중 7 개는 이전 Gitpaste-12 샘플에서도 찾아볼 수 있었다. 또한 오픈 Android Debug Bridge 커넥션 및 존재하는 악성코드 백도어를 해킹하려 시도한다."



[이미지 출처] https://blogs.juniper.net/en-us/threat-research/everything-but-the-kitchen-sink-more-attacks-from-the-gitpaste-12-worm

이 취약점 31 개 목록에는 2020 년 발견된 원격 코드 취약점인 F5 BIG-IP Traffic Management (CVE-2020-5902), Pi-hole Web (CVE-2020-8816), Tenda AC15 AC1900 (CVE-2020-10987), vBulletin (CVE-2020-17496), SQL 인젝션 취약점인 FUEL CMS (CVE-2020-17463)가 포함되어 있었다.

지난 10 월, Mirai 봇넷의 새로운 변종인 Ttint 가 DoS 공격, 악성 명령 실행, 원격 접근을 위한 리버스 셸 구현이 가능한 RAT 을 확산시키기 위해 CVE-2020-10987 을 포함한 Tenda 라우터 제로데이 취약점 2 개를 악용하고 있는 것이 발견되었다.

이 악성코드는 X10-unix 와 모네로 크립토마이닝 소프트웨어를 설치하는 것 이외에도 포트 30004 와 30006 을 리스닝하는 백도어를 오픈하고, 피해자의 외부 IP 주소를 개인 Pastebin 에 업로드하고, 포트 5555 에서 Android Debug Bridge 연결을 시도한다. 성공적으로 연결될 경우 안드로이드 APK 파일인 "weixin.apk"를 다운로드한다. 이는 X10-unix 의 ARM CPU 버전을 설치한다. Junipe 의 연구원들은 최소 100 개 이상의 호스트가 이 감염을 전파하고 있는 것으로 추정했다.

[출처] https://thehackernews.com/2020/12/wormable-gitpaste-12-botnet-returns-to.html
https://blogs.juniper.net/en-us/threat-research/everything-but-the-kitchen-sink-more-attacks-from-the-gitpaste-12-worm
https://blogs.juniper.net/en-us/threat-research/gitpaste-12

(주)이스트시큐리티

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