이스트시큐리티

보안 동향 보고서

No.139 2021.04

No.139 2021.04

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

2021년 3월에도 국내외에서 지속적인 APT 공격이 수행됨과 함께 다양한 신규 악성코드가 사이버 공격을 수행하는 정황이 포착되었습니다.

3월 초에는 유명 채팅 서비스인 '디스코드(Discord)'를 악용해 국내 포털의 '아이디 거래 계약서'를 사칭한 악성코드가 유포되었습니다. 악성코드가 포함된 악성 파일은 파일 확장자가 정상적인 문서처럼 보이지만 실제로는 .xls, .hwp 등 문서 확장자 뒤에 .exe, .scr과 같은 확장자가 숨겨진 2중 확장자명 위장 수법을 사용했습니다. 2중 확장자명 위장 수법은 윈도우 운영 체제가 '확장자명 숨김 처리'를 기본 설정으로 사용한다는 점을 악용한 것입니다. 사용자가 숨겨진 파일 확장자를 인지하지 못하고 정상 문서로 착각해 파일을 실행할 경우 추가 악성코드가 다운로드되어 PC 내부의 중요한 자료와 개인정보 유출 등의 피해를 입을 수 있습니다. 따라서 윈도우 운영 체제 사용자는 파일 확장자명을 확인할 수 있도록 윈도우 폴더 옵션을 변경하고 아이콘과 확장자를 꼼꼼히 살펴보고 접근하는 보안 습관이 중요합니다. 이와 관련하여 이스트시큐리티 시큐리티대응센터(ESRC)의 자세한 분석 내용이 궁금하시다면 알약 블로그 및 Threat Inside에서 확인하실 수 있습니다.

기업을 타깃으로 한 랜섬웨어 공격들이 끊이지 않고 있는 가운데, Sodinokibi, Clop 등을 비롯한 유명 RaaS (Ransomware-as-a-Service) 운영자들이 피해자들에게 랜섬머니 지불을 강요하기 위해 다양한 전략을 채택하고 있습니다. 최근 Sodinokibi 랜섬웨어는 피해자의 비즈니스 파트너에게 전화하는 전략을, Clop 랜섬웨어는 피해 기업의 고객에게 직접 랜섬웨어 감염 사실을 알리기 시작했습니다. 또한 랜섬웨어들은 감염된 PC의 파일을 암호화할 뿐만 아니라 암호화 작업 이전에 파일을 탈취하고 있어 기업들에게 더 큰 피해를 입히고 있습니다. 이러한 랜섬웨어 공격자들은 피해자가 랜섬머니를 지불하더라도 파일을 복호화해주지 않거나 탈취한 데이터를 삭제하지 않고 또다시 유포할 가능성이 있으므로 평소 인터넷 사용 습관에 주의하여 랜섬웨어에 감염되지 않는 것이 가장 중요합니다.

최근 유명 사이버 범죄 포럼에 전 세계 5.33억 명의 페이스북 사용자의 개인정보가 무료로 유출되었으며 이 중 한국인 12 만 명의 개인정보도 포함되어 큰 이슈가 되었습니다. 이에 페이스북은 2019 년에 이미 유출된 데이터로 데이터가 유출된 경로로 악용된 취약점은 이미 패치가 된 상태라고 밝혔습니다. 하지만 여전히 해커 포럼에서 유출된 데이터에서 접근이 가능한 만큼 공격자들이 해당 데이터를 이용하여 피싱, 스미싱 등의 추가 공격을 수행할 가능성이 존재합니다. 따라서 사용자는 이용 중인 사이트의 비밀번호를 주기적으로 변경하고 가급적 각 사이트 별로 다른 비밀번호를 사용하는 것이 좋습니다.

최근 공격자들이 지속적으로 공격 기능을 고도화하고 공격 범위를 확대해 가는 모습을 보여주고 있습니다.
항상 공격자들은 공격 목표로 삼는 타깃이 어떤 부분에 관심을 가지고 있는지 집중합니다. 내가 평소에 관심을

01 악성코드 통계 및 분석

가지고 있는 주제에 대한 내용이라고 할지라도 출처를 알 수 없는 메일을 열람하거나 신뢰할 수 없는 앱을 PC나 스마트폰에 설치하는 것은 최대한 지양해야 하며 사용하는 PC 및 모바일 기기의 운영 체제에 맞는 백신을 통해 사용 환경을 항상 점검할 것을 권장합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021 년 3 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Hosts.media.opencandy.com 와 Misc.HackTool.AutoKMS 이 각각 1 위와 2 위를 차지했으며 JS:Trojan.Cryxos.5175 를 비롯한 4 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 눈에 띄는 부분으로는 Trojan.Agent.Gen 이 7 계단 하락하여 10 위를 차지했으며, 그 외에는 큰 순위 변동 없이 대체적으로 지난달과 유사한 순위 양상을 보였다.

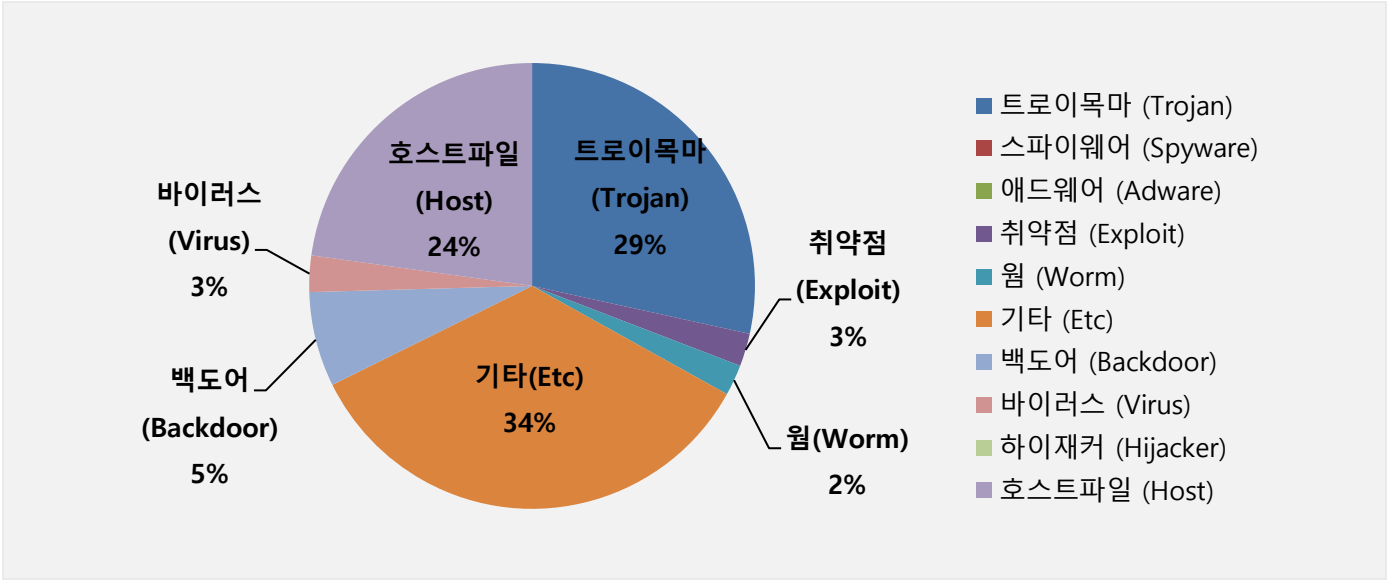
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	669,543
2	-	Misc.HackTool.AutoKMS	ETC	399,168
3	↑ 2	Trojan.ShadowBrokers.A	Trojan	339,999
4	↑ 2	Misc.HackTool.KMSActivator	ETC	200,098
5	New	JS:Trojan.Cryxos.5175	Trojan	193,449
6	↓ 2	Backdoor.Generic.792814	Backdoor	154,790
7	↑ 2	Misc.Riskware.Segurazo	ETC	152,091
8	↓ 1	Misc.Keygen	ETC	120,270
9	New	JS:Trojan.Cryxos.5275	Trojan	107,357
10	↓ 7	Trojan.Agent.Gen	Trojan	105,445
11	↓ 3	Misc.Riskware.TunMirror	ETC	101,655
12	↓ 2	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	87,860
13	New	Win32.Neshta.A	Virus	73,868
14	New	Exploit.CVE-2010-2568.Gen	Exploit	72,906
15	↓ 1	Worm.ACAD.Bursted	Worm	68,846

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 03 월 01 일 ~ 2021 년 03 월 31 일

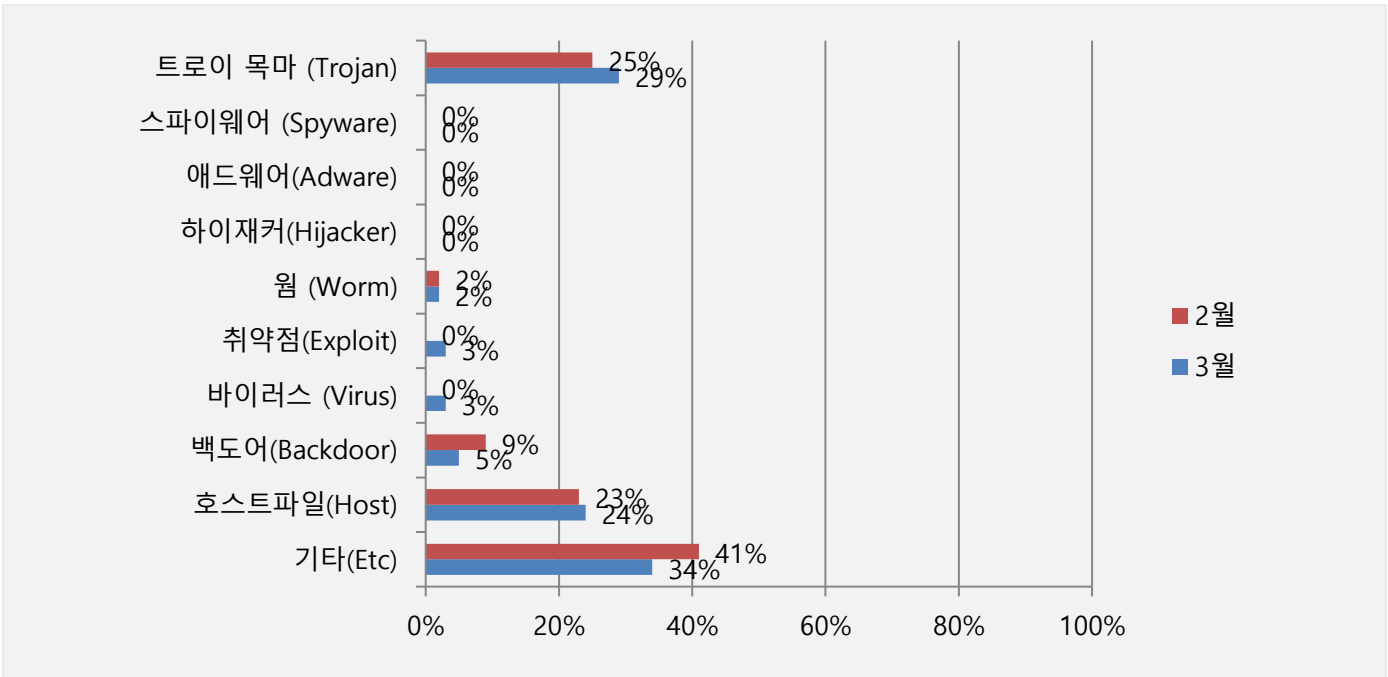
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 34%를 차지했으며 트로이목마(Trojan) 유형이 29%로 그 뒤를 이었다. 지난달 기타 유형을 제외하고 두 번째로 많은 비중을 차지했던 호스트파일(Host) 유형이 24%로 소폭 증가했으며, 지난달 감염 악성코드 TOP 15 에 오르지 못했던 취약점(Exploit) 유형과 바이러스(Virus) 유형이 이번 달에는 각각 3%, 3%를 기록했다. 2021 년 2 월과 비교하여 전체 감염 건수는 약 17.97% 증가하였다.



카테고리별 악성코드 비율 전월 비교

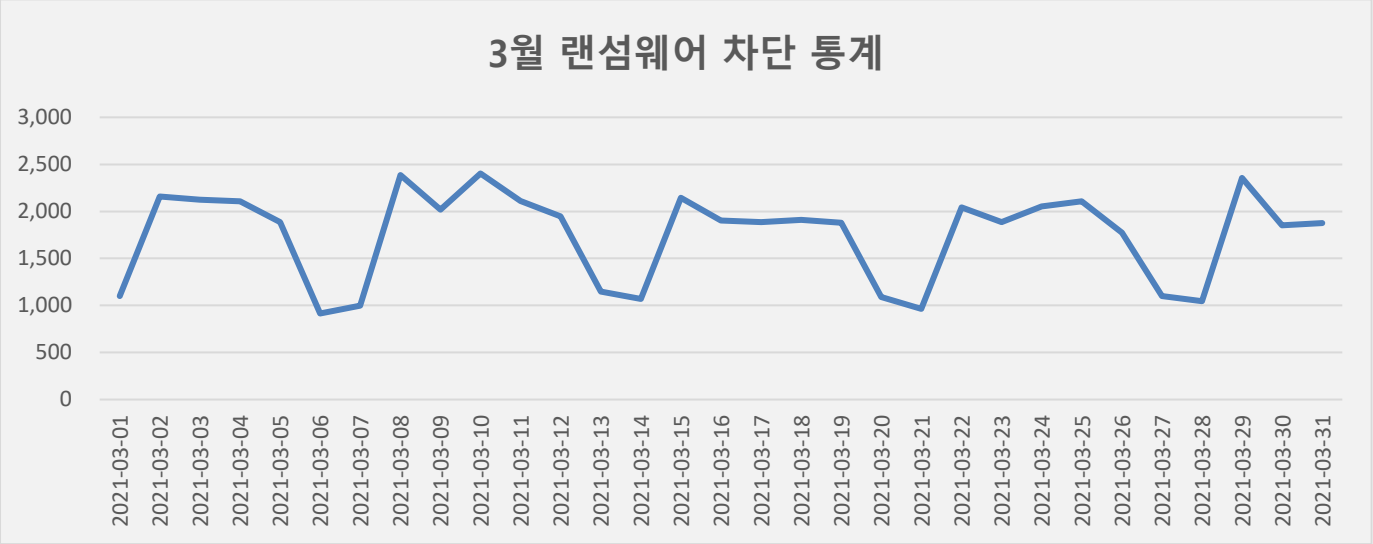
3 월에는 지난 2 월과 비교하여 트로이목마(Trojan) 유형이 4% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 1%를 증가했다. 또한 지난 달에는 탐지되지 않았던 바이러스(Virus) 유형과 취약점(Exploit) 유형의 수치가 증가하여 두 유형 모두 3%를 기록했다. 2 월에 9%를 차지했던 백도어(Backdoor) 유형이 소폭 감소하여 5%를 기록했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

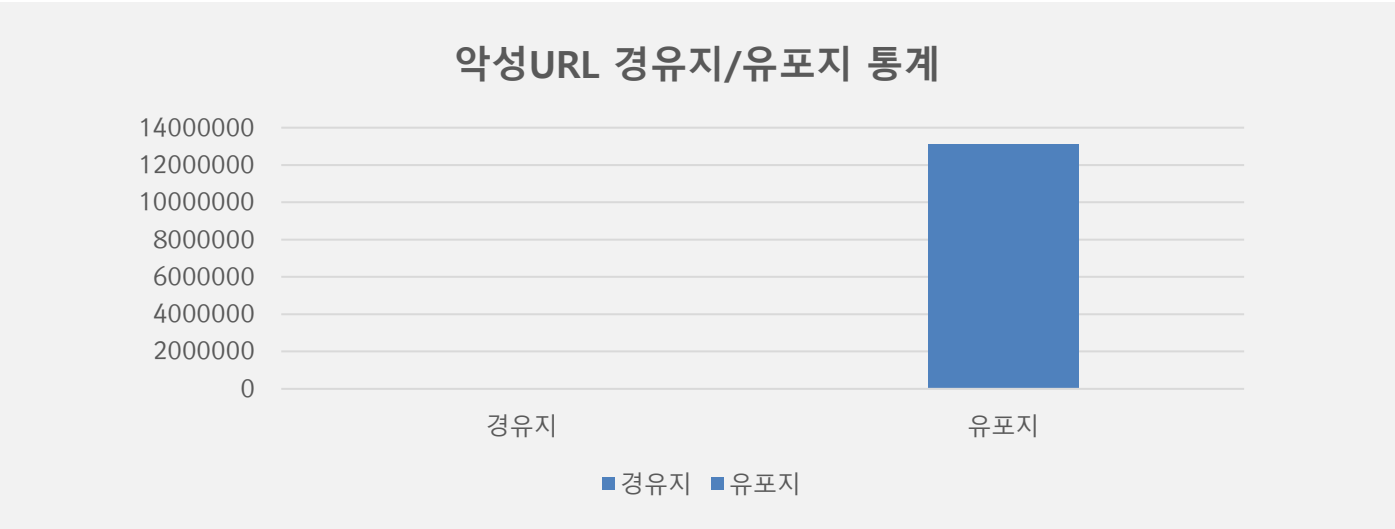
3 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 3 월 1 일부터 3 월 31 일까지 총 54,250 건의 랜섬웨어 공격 시도가 차단되었다. 2 월에 비해 랜섬웨어 공격 건수인 46,182 건에 비해 약 17.47% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 3 월 한 달간 총 13,167,607 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 2 월 한 달간 확인되었던 13,336,133 건의 악성코드 경유지/유포지 URL 수에 비해 약 1.28% 가량 감소한 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. 알약 1 분기 랜섬웨어 행위기반 차단 건수: 154,887 건!

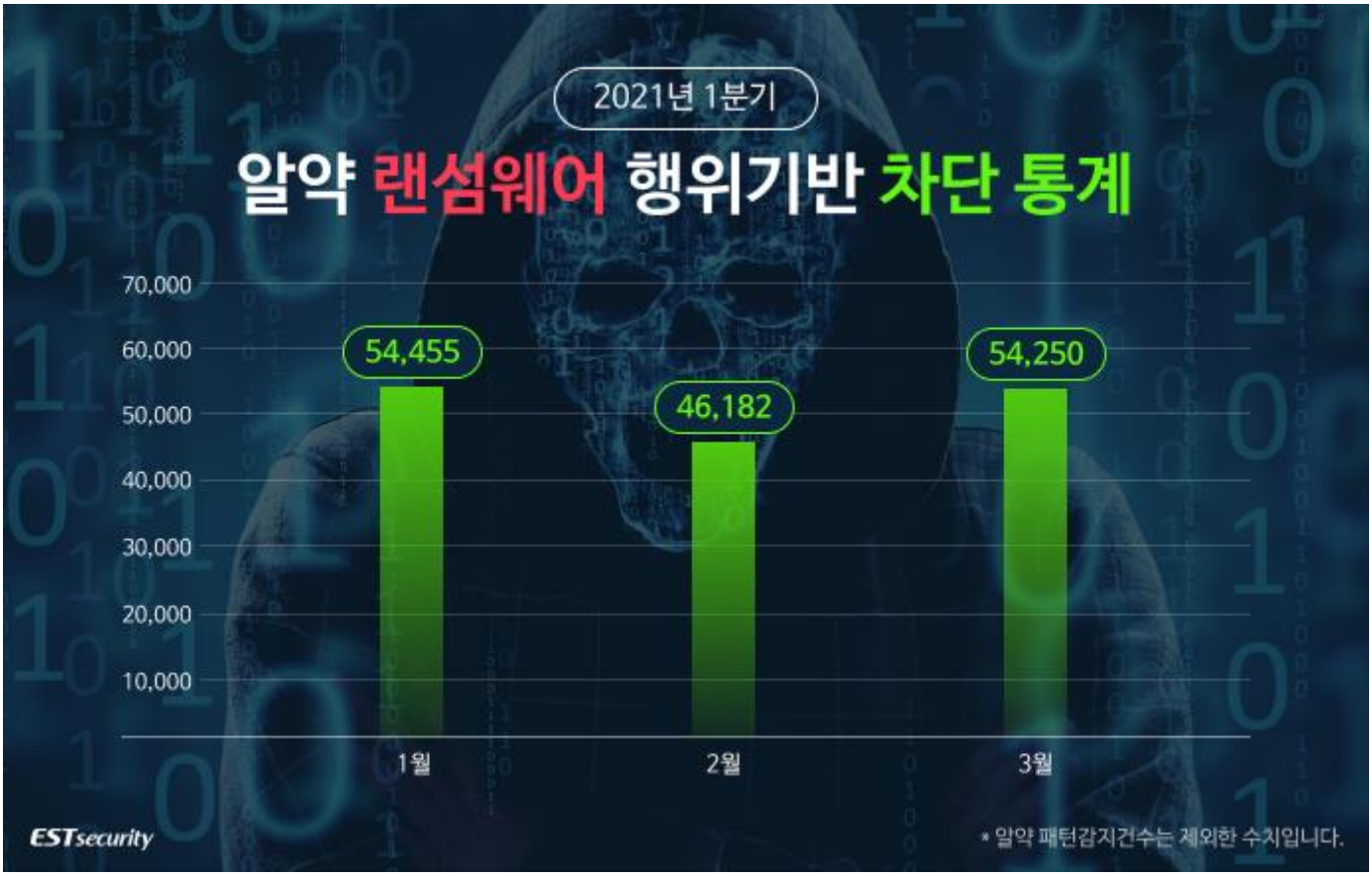
2. 트레소리트(Tresorit) 클라우드 서비스를 이용한 Formbook 악성 이메일 주의!!

1. 알약 1 분기 랜섬웨어 행위기반 차단 건수: 154,887 건!

2021 년 1 분기, 알약을 통해 총 154,887 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, 2021 년 1 분기 알약을 통해 차단된 랜섬웨어 공격은 총 154,887 건으로, 이를 일간 기준으로 환산하면 일 평균 약 1,720 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다. 다만, 2019 년부터 현재까지 약 2 년에 걸쳐 전체 랜섬웨어 공격 건수는 지속적으로 감소하는 추세를 보이고 있습니다.



[그림] 알약 랜섬웨어 행위기반 차단 기능'을 통해 차단된 2021 년 1 분기 랜섬웨어 공격 통계]

02 전문가 기고

ESRC 는 2021 년 1 분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

1) MS Exchange Server 취약점 악용하는 DearCry, Black Kingdom 랜섬웨어 등장
2) 국내 유명 자동차 제조 기업, 랜섬웨어 공격으로 데이터 유출 피해 발생
3) '비너스락커' 그룹이 유포하는 Makop 랜섬웨어 공격 꾸준히 발생
4) Emotet, Netwalker 랜섬웨어 무력화 및 Ziggy 랜섬웨어 운영 종료

2021 년 1 분기에는 이메일 내 입사 지원서, 이력서, 포트폴리오 등으로 위장한 첨부파일 형태로 유포되는 Makop 랜섬웨어가 꾸준히 상위권을 유지했으며, 랜섬 머니 지불을 강요하기 위해 DDoS 공격 및 언론인과 피해자의 사업 파트너에게 음성 전화를 시도하는 등 새로운 전략을 추가한 Sodinokibi 랜섬웨어 공격이 등장했습니다. 또한 랜섬웨어 공격 건수는 지난해 4 분기에 비해 전반적으로 감소 추세를 나타냈습니다.

1 분기에 주목할만한 위협으로는 지난 3 월에 등장한 DearCry, Black Kingdom 랜섬웨어가 눈에 띕니다. 3 월 초부터 이슈가 되고 있는 Microsoft Exchange 서버의 'ProxyLogon' 취약점(CVE-2021-26855)를 악용하며 미국, 캐나다, 영국, 독일, 호주 등 전 세계 다양한 국가를 타깃으로 공격을 감행하고 있습니다.

또한 Doppelpaymer 랜섬웨어 그룹이 현대기아자동차의 기업 내부 자료를 다크웹에 대거 공개했습니다. Doppelpaymer 해커들이 운영하는 다크웹 사이트에는 실제로 현대기아차를 비롯해 현대글로비스 등 관련 계열사 데이터가 대거 발견되었고, 해당 데이터에는 제니시스 자동차 도면, 기업 재무 자료, 내부 직원 아웃룩 이메일 백업 파일 등 민감한 문서들도 포함되었습니다. Doppelpaymer 운영자들은 거액의 협상 금액을 제시하며 탈취한 대규모 내부 정보를 다크웹에 유출하겠다고 협박했으며, 기아차 미국 법인에서는 IT 서비스 장애가 며칠간 지속되었습니다.

1 월부터 3 월까지 비너스락커 그룹이 유포하는 Makop 랜섬웨어도 꾸준히 발견되었습니다. Makop 공격자 들은 주로 입사지원서, 이력서, 경력 사항, 포트폴리오 또는 이미지 저작권 관련 문서로 위장한 EXE 파일을 첨부한 스피어피싱 이메일 형태로 랜섬웨어를 유포했으며, 기존에 주로 사용하던 HWP, PDF 방식에서 Word 아이콘으로 변경하고, 암호화 파일에 추가하는 확장명을 변경해가며 탐지망을 교묘히 피해가는 수법을 보이고 있습니다.

2021 년 1 분기에는 또한 여러 국제 수사 기관들의 공조로 Netwalker 랜섬웨어와 Emotet 등 유명 악성코드 조직이 무력화되었으며, 이로 인해 Ziggy 랜섬웨어 운영자들이 스스로 운영을 중단하겠다 선언하고 피해자들에게 복호화 키를 공개하기도 했습니다.

이 밖에도 첫 기업용 랜섬웨어인 Babuk Locker 가 발견되었으며, 웜 기능을 갖춘 Ryuk 랜섬웨어 변종이 발견되었습니다. 2021 년부터 새롭게 활동을 시작한 Babuk Locker 는 피해자에 따라 고유 확장자, 랜섬노트, Tor URL 등을 달리 하였고, 안전한 암호화 알고리즘을 사용해 파일 복구를 방지했습니다. 또한 피해자로부터 탈취한 데이터를 유출하겠다고 협박하는 이중 갈취 전략을 사용하며, 데이터 유출을 위한 사이트도 개설 하겠다는 계획도 밝혔습니다. 3 월에 발견된 Ryuk 랜섬웨어의 새로운 변종에는 웜 기능이 포함되어, 피해자의 로컬 네트워크 내에 있는 다른 장치로 확산이 가능합니다. 전파는 실행 파일을 식별된 네트워크 공유에 복사하는 방법으로 이루어지며, 원격 시스템에서 예약 작업을 생성해 해당 프로세스를 지속적으로 반복합니다.

02 전문가 기고

ESRC 센터장 문종현 이사는 “2021 년 1 분기 내 유포된 랜섬웨어 중 비너스락커 조직이 Makop 랜섬웨어를 지속 활용한 정황이 수십 차례 포착된 바 있다."고 언급하며, “랜섬웨어 공격 양상이 기존의 공격 방식에서 새로운 기능을 추가하거나 여러 공격 기법을 결합한 형태로 점점 진화하고 있기 때문에 관련 기업과 개인들은 주기적인 백업 및 안전한 보안 시스템 구축 등을 통해 미리 대비하는 자세가 필요하다."고 강조했습니다.

이밖에 ESRC 에서 밝힌 2021 년 1 분기에 새로 발견되었거나, 주목할만한 랜섬웨어는 다음과 같습니다.

랜섬웨어 명	주요 내용
Babuk Locker	주로 기업 피해자를 노리는 '사람이 운영하는(human-operated)' 랜섬웨어로, 확장 프로그램, 랜섬노트, Tor URL 이 피해자 별로 커스텀되어 있음. 코딩 형태가 전문적이지는 않지만, Elliptic-curve Diffie-Hellman 알고리즘이 포함된 안전한 암호화를 사용해 피해자가 파일을 무료로 복호화할 수 없도록 예방함.
DearCry	Microsoft Exchange 서버의 ProxyLogon 취약점을 악용하는 랜섬웨어로, 설치된 후 ‘msupdate’라는 비정식 윈도우 서비스 종료를 시도함. 파일 암호화를 위해 AES-256 및 RSA-2048 을 사용하며, 암호화된 각 파일의 시작 부분에 'DEARCRY!' 문자열을 추가함.
Black Kingdom	DearCry 랜섬웨어와 마찬가지로, Microsoft Exchange 서버의 ProxyLogon 취약점을 악용하는 랜섬웨어로, Pulse VPN 취약점을 악용하여 기업 네트워크를 해킹한 공격에도 사용된 바 있으며, 윈도우 실행파일로 컴파일된 Python 스크립트가 랜섬웨어 파일로 사용됨.
HelloKitty	비디오 게임 업체, 전력 회사, IT 서비스 기업 등을 노리는 랜섬웨어로, 탈취한 데이터 유출을 빌미로 사용자를 협박하는 이중 갈취 전략을 사용함. 랜섬노트에 피해 기업명, 개인정보, 탈취된 데이터 양 등의 정보가 포함되며, 랜섬 지불 기한을 1-2 일로 제한하여 빠른 랜섬 지불을 유도하고 피해자의 추가 대응을 방지함.
Vovalex	Ccleaner 시스템 최적화 프로그램의 설치 파일로 위장하여 유포되는 랜섬웨어로, 디지털 서명이 포함된 정상 설치 파일을 사용해 사용자를 속이며, 랜섬노트에는 영어와 러시아어를 사용해 모네로(XMR) 암호화폐를 지불하도록 요구함.
Ziggy	최근 운영을 중단하고 피해자에게 복호화 키 공개 및 랜섬 머니를 환불한 랜섬웨어로, SQL 파일 내 포함된 키를 사용할 수 있는 복호화 툴을 공개했으며, 피해자에게 지정 이메일 주소를 통해 비트코인 결제 증빙 등 랜섬 지불 내역을 보낼 것을 안내함.
Ryuk	로컬 네트워크를 통해 자가 확산되는 웜 기능을 갖춘 새로운 변종으로 재등장한 랜섬웨어로, 실행되면 윈도우 RPC 접근이 가능한 모든 기기에 자기 자신을 확산시킴. 실행 파일을 식별된 네트워크 공유에 복사하는 방법으로 전파가 이루어지며, 예약 작업 생성을 통해 지속성을 확보함.
Sodinokibi	최근 피해자의 랜섬 지불을 강요하기 위해 DDoS 공격 및 언론인과 피해자의 비즈니스 파트너에게 음성 통화를 수행하겠다고 협박하는 전략을 추가한 랜섬웨어로, 홈페이지에 랜섬웨어 제휴 파트너에게 3 계층과 7 계층 DDoS 공격을 수행할 수 있는 유료 서비스를 제공한다고 안내함.
DeroHE	윈도우 유틸리티 개발 업체 IObit 포럼으로 위장해 유포되는 랜섬웨어로, ZIP 첨부파일에는 디지털 서명된 합법적인 IObit 라이선스 관리자 프로그램 파일을 포함시키며, DLL 파일을 서명되지 않은 악성 버전으로 바꿔치기 하는 방법으로 공격을 수행함.

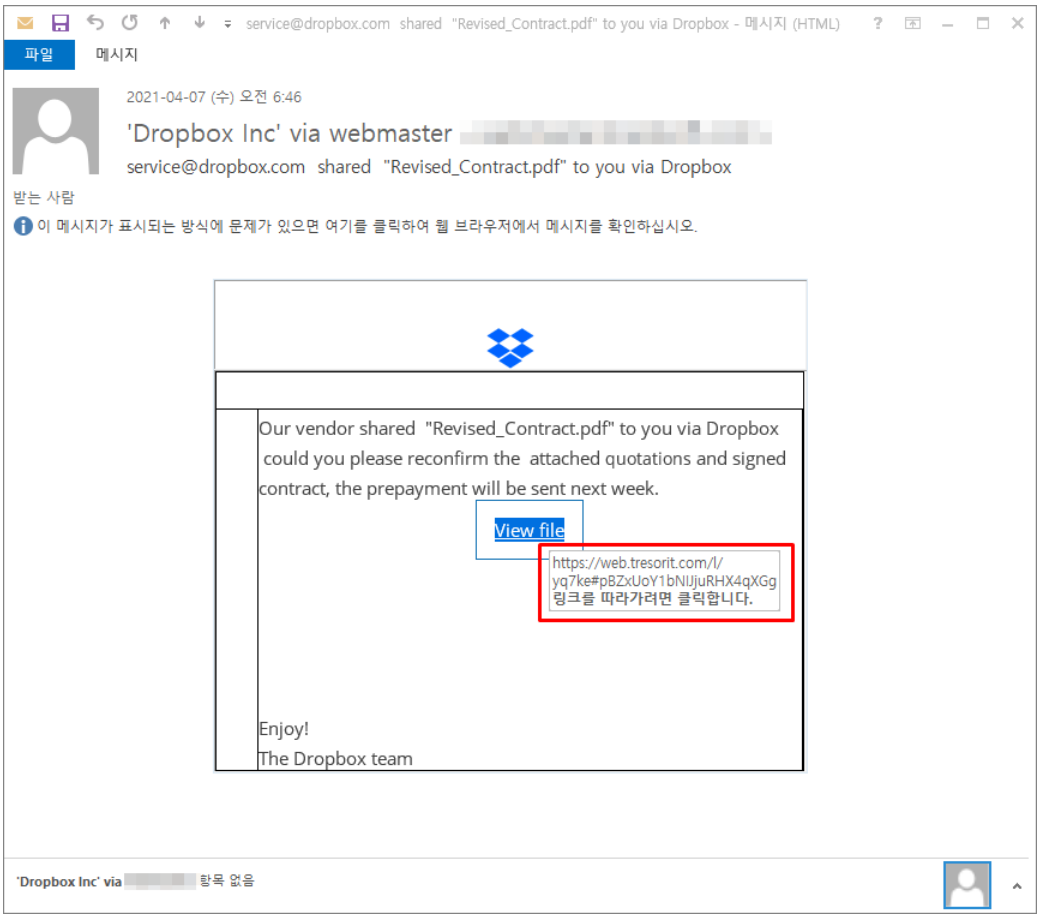
랜섬웨어 유포 케이스의 대다수는 이메일 형태지만, 코로나 19 바이러스 확산 방지를 위해 재택 근무를 수행 하는 임직원이 증가함에 따라 기업 내부망 접속을 위해 사용되는 재택 근무 단말기 OS/SW 보안 업데이트 점검을 의무화하고 임직원 보안 인식 교육도 병행해야 합니다.

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. 트레소리트(Tresorit) 클라우드 서비스를 이용한 Formbook 악성 이메일 주의!

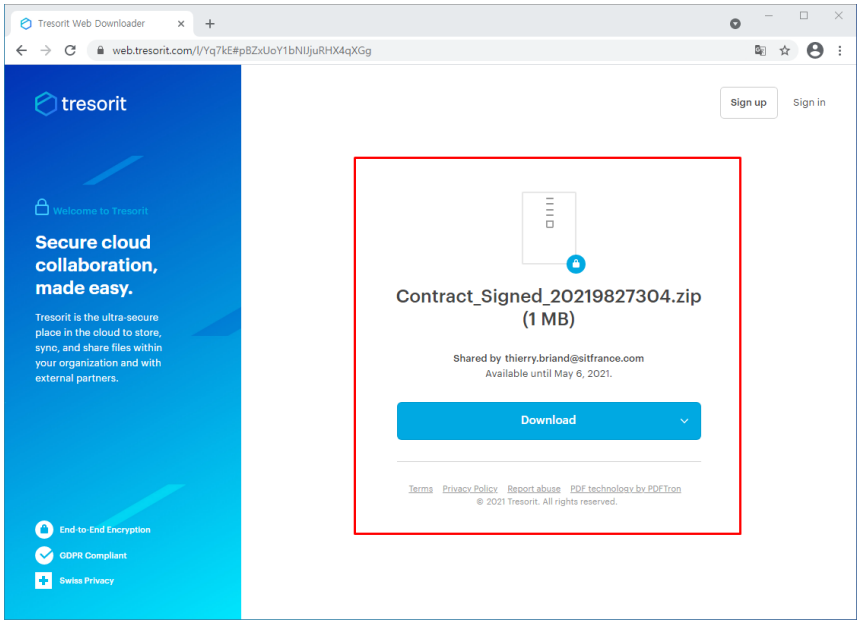
대표적인 클라우드 서비스 트레소리트(Tresorit)를 이용한 Formbook 악성파일이 유포 중인 정황이 발견되어 사용자들의 주의가 필요합니다.

이번에 발견된 악성메일은 "service@dropbox.com shared "Revised_Contract.pdf" to you via Dropbox" 이라는 제목으로 수신되었으며, 본문에 기재된 Dropbox 링크를 통해 허위 견적서 파일을 다운로드하도록 유도합니다.



[그림 1] 견적서로 위장 된 악성 이메일 화면

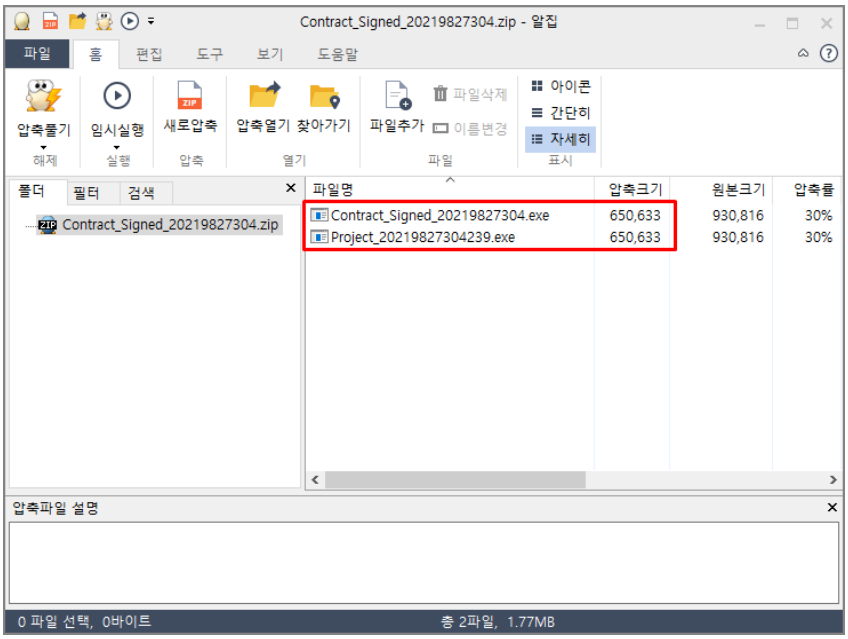
메일 본문에 기재된 링크는 Dropbox 가 아닌 Tresorit 서비스 링크로 연결되며, Formbook 악성 파일이 담긴 압축파일을 다운로드할 수 있습니다.



[그림 2] Tresorit 서비스에 업로드 된 악성코드 화면

Contract_Signed_20219827304.zip 파일 내부에는 2 개의 파일이 포함되며, 파일명만 다른 동일한 해쉬를 가진 파일입니다.

- Contract_Signed_20219827304.exe
- Project_20219827304239.exe



[그림 3] 압축파일 내부 화면

사용자가 압축 파일을 해제하여 실행할 경우, 시스템 정보, 브라우저 크리덴셜 정보, 현재의 화면 스크린샷, 시스템 종료/재시작, 추가 다운로드 기능들을 수행하는 Formbook 악성코드가 동작하게 됩니다.

- C2 정보 : hxxp://www[.]sainworks[.]com/nyk/

```
CreateCompatibleDC = v4->CreateCompatibleDC;
v51 = v6;
v50 = CreateCompatibleDC(v6);
if ( !v50 )
  return 0;
v8 = a2;
v9 = a3;
v49 = &v20;
if ( !a2 || !a3 )
{
  GetSystemMetrics = v4->GetSystemMetrics;
  v49 = &v26;
  v8 = (GetSystemMetrics)(0);
  v9 = (v4->GetSystemMetrics)(1);
}
v11 = (v4->CreateCompatibleBitmap)(v51, v8, v9);
v48 = v11;
if ( v11 )
{
  (v4->SelectObject)(v50, v11, v16);
  if ( a4 )
  {
    v12 = (v4->GetSystemMetrics)(1);
    v13 = (v4->GetSystemMetrics)(0, v12);
    (v4->StretchBlt)(v50, 0, 0, v8, v9, v51, 0, 0, v13);
```

[그림 4] 현재 화면을 스크린샷으로 저장하는 코드 화면

```
switch ( v14 )
{
  case 53:                                  // Delete Cookies
    if ( **(a1 + 2872) == 0x474E4246 )
    {
      sub_404D20(a1);
      return 0;
    }
    return 0;
  case 54:                                  // Shutdown and Restart
    if ( **(a1 + 2872) == 0x474E4246 )
    {
      sub_404560(a1, 18);
      return 0;
    }
    return 0;
  case 55:                                  // ShutDown and PowerOff
    if ( **(a1 + 2872) == 0x474E4246 )
      sub_404560(a1, 24);
    return 0;
  case 56:                                  // 크리덴셜 정보 탈취
    if ( **(a1 + 2872) == 0x474E4246 )
      sub_4048A0(a1);
    return 0;
```

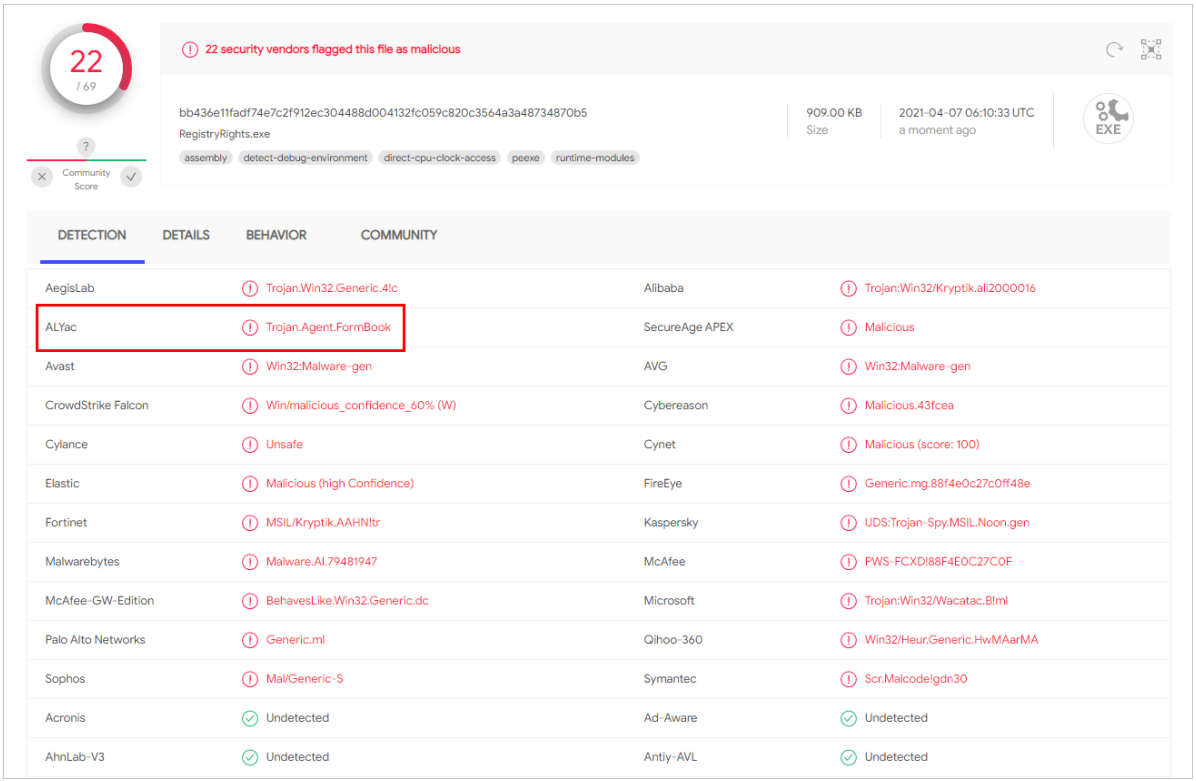
[그림 5] 명령 제어 기능을 수행하는 코드 화면

Formbook 은 정보 수집 및 명령 제어 기능을 수행하는 악성코드로 초기부터 현재까지 유사한 코드로 동작하고 있기때문에 Formbook 에 대한 상세 분석은 아래 링크에서 확인하실 수 있습니다.

Trojan.Agent.FormBook 악성코드 분석 보고서

이와 같이 출처가 불분명한 메일에 기재된 링크는 실행하지 않은 것이 좋으며, 백신의 실시간 감시를 사용하고, 정기적인 검사를 습관화하여야 합니다.

현재 알약에서는 'Trojan.Agent.FormBook' 탐지 명으로 탐지 중입니다.

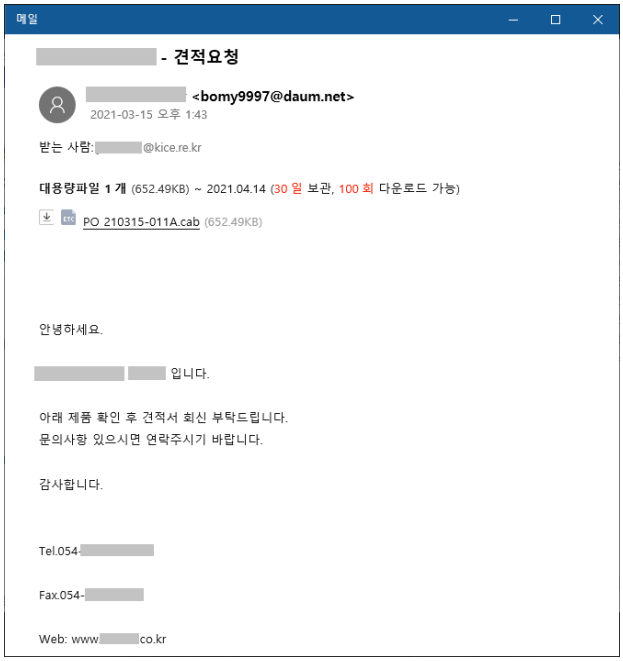


[그림 6] 바이러스토탈 ALYac 탐지 화면

03
악성코드 분석 보고

[Spyware. Lokibot] 악성코드 분석 보고서

Lokibot은 인포스틸러 악성코드로서 웹 브라우저, 메일 클라이언트, FTP 클라이언트 등 감염 PC에 설치된 다양한 프로그램들에서 크리덴셜 정보를 탈취하는 기능을 가지고 있다. 수 년 전부터 꾸준히 유포되고 있는 악성코드이지만 현재까지도 꾸준히 배포되고 있다. Lokibot 은 대부분 피싱메일을 통해 유포되고 있으며, 진단을 우회하기 위해 요즘은 주로 닷넷(.NET) 프로그램의 형태로 유포되고 있다.



[그림] 견적 요청 위장 피싱메일

Lokibot 악성코드는 주로 견적 요청과 같은 피싱메일로 유포되며, 닷넷(.NET) 패커로 제작되어 있으며, Lokibot 페이로드를 자식프로세스에 인젝션하여 동작하며, 여러 종류의 수집 대상 프로그램에서 저장하고 있는 크리덴셜 정보를 탈취하는 것을 주목적으로 한다.

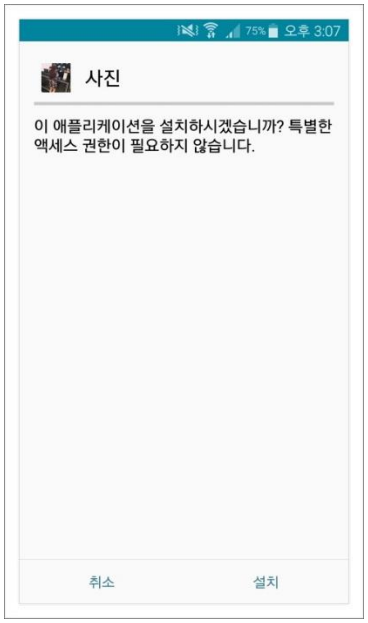
개인보다는 기업체를 타깃으로 하기 때문에 업무용으로 사용하는 PC 의 크리덴셜 정보가 유출되면 더 큰 피해가 발생될 수 있어 주의가 필요하다.
따라서, 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 혹은 URL 클릭을 삼가야 하며, 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 해당 악성코드를 'Spyware.Lokibot' 탐지 명으로 진단하고 있으며, 관련 상세분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Agent] 악성코드 분석 보고서

몸캠피싱 공격은 스마트폰 채팅 어플 등을 통해 피해자를 찾는 것으로 시작된다. 이후 채팅을 통해 피해자의 호감을 산 뒤 공격자는 음란 화상 채팅을 유도한다. 이때 공격자는 피해자의 음란 행위를 녹화한다.

그리고 피해자의 스마트폰에 악성 앱 설치를 유도하여 피해자가 악성 앱 설치를 하면 연락처 등의 개인 정보를 탈취한 후 음란행위 영상을 지인에게 유포하겠다는 협박을 통해 금전을 갈취하는 것으로 공격을 마무리한다.



[그림] 설치 시 화면

몸캠피싱은 피해자의 금전 갈취를 주요 목적으로 하고 있다. 공격자는 금전 갈취라는 목적을 위해 Spyware.Android.Agent 악성 앱을 수단으로 활용하고 있는 것이다.

몸캠피싱 공격은 사용자의 예방 노력이 무엇보다 중요하다. 악성 앱 설치 시 피해자는 금전적인 손해와 더불어 심적인 고통을 지속적으로 받을 수 있기 때문이다. 따라서 제 3 자의 권유로 인한 앱의 설치 시 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 'Spyware.Android.Agent' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

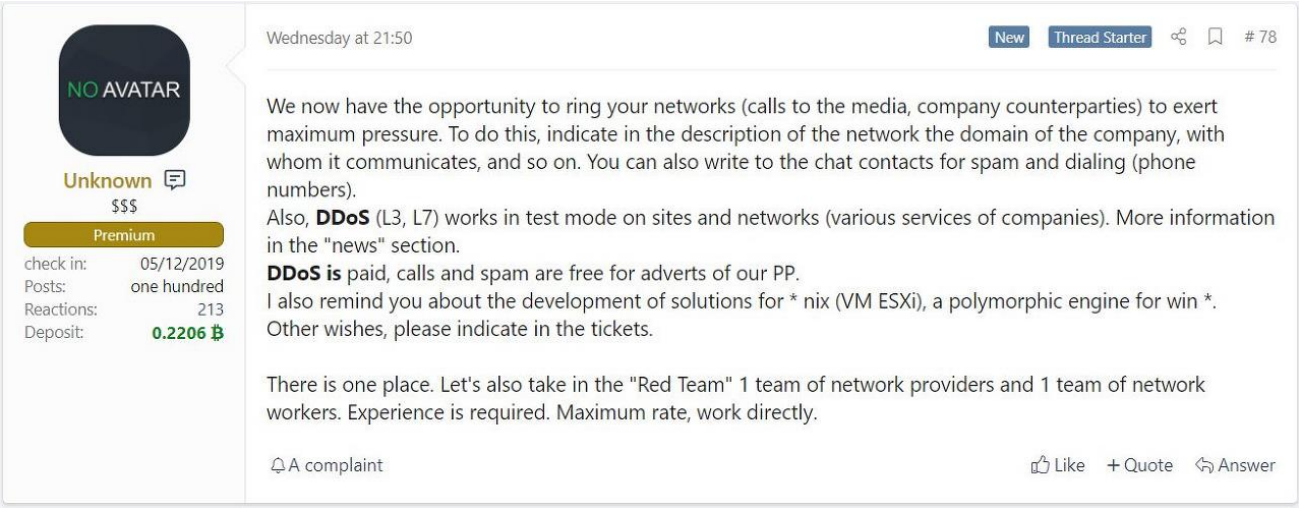
Sodinokibi 랜섬웨어 그룹, 피해자의 사업 파트너에게 전화하는 전략 추가해

Ransomware gang plans to call victim's business partners about attacks

Sodinokibi 랜섬웨어 운영자가 피해자가 랜섬머니를 지불하도록 협박하기 위해 DDoS 공격 및 언론인과 피해자의 사업 파트너에게 음성 전화를 진행할 것이라 공지했다. Sodinokibi 는 서비스형 랜섬웨어(RaaS)로 랜섬 웨어 운영자가 악성코드 및 결제 사이트를 개발하고, 파트너들이 기업 네트워크를 해킹하여 랜섬웨어를 배포 하는 방식을 사용한다. 이 거래를 통해 Sodinokibi 개발자는 랜섬머니의 20%~30%를 가지고 파트너는 나머지 70~80%를 가져간다. 피해자가 랜섬머니를 지불하도록 압력을 가하기 위해, 랜섬웨어 운영자들은 피해자가 랜섬머니를 지불하지 않을 경우 그들이 훔친 암호화되지 않은 파일을 공개하겠다고 협박하는 '이중 협박' 전략을 사용하기 시작했다.

- 이제 VOIP 통화 및 DDoS 공격까지 실행할 예정

지난 2 월, Sodinokibi 랜섬웨어는 DDoS 공격을 수행하고, 피해자 및 그들의 파트너에게 VOIP 전화를 사용 하여 연락할 사람을 구하는 구인 공고를 게시했다. 그리고 오늘, 3xp0rt 로 알려진 한 보안 전문가는 Sodinokibi 가 랜섬웨어 파트너가 피해자를 더욱 압박하는데 사용할 수 있는 새로운 전략을 사용하기 시작했다고 밝혔다. 이 새로운 전략은 공격자, 협력 파트너가 음성 변환된 VOIP 전화를 통해 언론과 피해자의 사업 파트너에 공격 관련 정보를 알리는 무료 서비스를 포함한다. 이 랜섬웨어 그룹은 기업들에게 공격 중 데이터가 노출된 사실을 파트너에게 알리겠다고 협박할 경우 피해자가 랜섬머니를 지불하도록 더 큰 압박을 줄 수 있을 것이라 생각한 것으로 보인다. 또한 Sodinokibi 는 제휴 파트너가 3 계층 및 7 계층 DDoS 공격을 수행할 수 있는 유료 서비스를 제공하고 있다.



[그림] Sodinokibi 의 새로운 협박 기능을 알리는 공지

[이미지 출처] https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/

3 계층 공격은 회사의 인터넷 연결을 중단시키는 데 사용되며, 7 계층 공격을 통해 웹서버와 같이 공개적으로 접근이 가능한 애플리케이션을 중단시킬 수 있다. 지난 10 월, SunCrypt 와 Ragnar Locker 랜섬웨어 운영자는 피해자들

이 랜섬머니를 지불하도록 압박하기 위해 DDoS 공격을 실행하기 시작했다. 2021 년 1 월, Avaddon 랜섬웨어 그룹 또한 이 전략을 사용하기 시작했다. 피해자에게 VOIP 전화를 통해 협박하는 수법은 수 많은 랜섬웨어 작업에서 사용되었지만, Bleeping Computer 측에서는 아직까지 언론사나 피해자의 사업 파트너에게 전화한 사례는 없었다고 밝혔다.

[출처] https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/

DearCry 랜섬웨어, 마이크로소프트 익스체인지 서버 노려

New DEARCRY Ransomware is targeting Microsoft Exchange Servers

공격자들이 ProxyLogon 제로데이 취약점을 악용하여 마이크로소프트 익스체인지(Exchange) 서버를 해킹한 후 'DearCry' 랜섬웨어를 설치하고 있는 것으로 나타났다. 마이크로소프트는 2021 년 3 월 초 공격자들이 새로운 제로데이 취약점인 ProxyLogon 을 악용하여 마이크로소프트 익스체인지 서버를 해킹하고 있다는 사실을 공개했다. 당시 공격자들이 이 취약점을 랜섬웨어를 배포하는데 악용할 것이라는 우려가 있었다. 그러한 우려는 현실이 되었으며 공격자들은 실제 공격에 이 취약점을 악용하여 DearCry 랜섬웨어를 배포하기 시작했다.

- DearCry 랜섬웨어

ID-Ransomware 의 Michael Gillespie 에 따르면 3 월 9 일을 시작으로 사용자들은 새로운 랜섬웨어의 랜섬노트 및 암호화된 파일을 업로드하기 시작했다. 해당 내용을 검토한 결과, 거의 모든 파일이 마이크로 소프트 익스체인지 서버에서 왔음을 발견했다. 마이크로소프트는 마이크로소프트 익스체인지 서버를 노린 ProxyLogon 취약점을 악용한 공격을 통해 DearCry 랜섬웨어가 설치되었음을 확인했다.

[이미지 출처] https://twitter.com/phillip_misner/status/1370197696280027136

MalwareHunterTeam 은 VirusTotal 에서 이 랜섬웨어의 샘플 3 개를 찾을 수 있었다. 이 파일은 모두 MingW 로 컴파일된 실행파일이었다. Bleeping Computer 에서 분석한 샘플 중 하나는 다음의 PDB 경로를 포함했다.

- C:\Users\john\Documents\Visual Studio 2008\Projects\EncryptFile – svcV2\Release\EncryptFile.exe.pdb

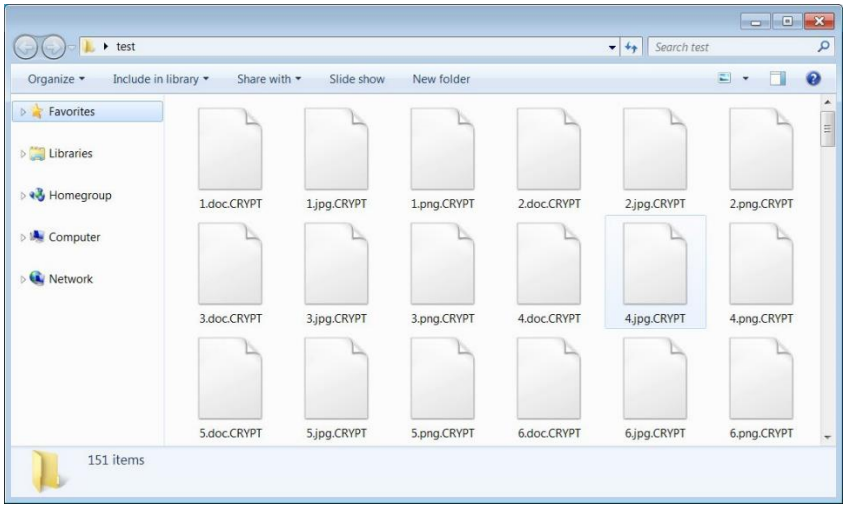
Advanced Intel 의 Vitali Kremez 에 따르면 DearCry 랜섬웨어는 시작된 후 'msupdate'라는 윈도우 서비스를 종료하려 시도한다. 이 서비스가 어떤 기능을 수행하는지는 아직까지 알려지지 않았지만, 정식 윈도우 서비스는 아닌 것으로 추정된다.

```
6  void *v3; // esi@2
7
8  result = OpenSCManagerA(0, 0, 0xF003Fu);
9  v1 = result;
10 if ( result )
11 {
12   v2 = OpenServiceA(result, "msupdate", 0xF01FFu);
13   v3 = v2;
14   if ( v2 )
15   {
16     DeleteService(v2);
17     ServiceStatus.dwCurrentState = 1;
18     ServiceStatus.dwControlsAccepted = 1;
19     ServiceStatus.dwWin32ExitCode = 0;
20     ServiceStatus.dwWaitHint = 0;
21     ServiceStatus.dwCheckPoint = 0;
22     SetServiceStatus(hServiceStatus, &ServiceStatus);
23     CloseServiceHandle(v3);
24     result = (SC_HANDLE)CloseServiceHandle(v1);
25   }
26   else
27   {
28     result = (SC_HANDLE)CloseServiceHandle(v1);
29   }
30 }
31 return result;
32 }
```

[그림] Msupdate 서비스를 종료하는 코드

[이미지 출처] https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

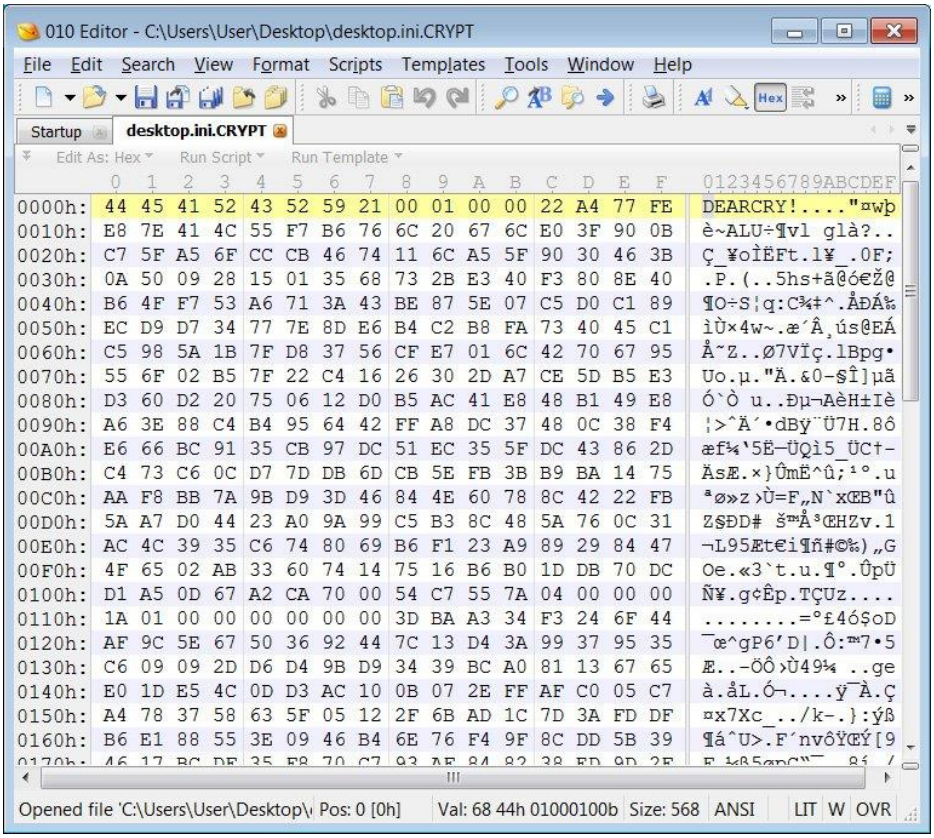
그런 다음 랜섬웨어는 컴퓨터의 파일을 암호화하기 시작한다. 파일을 암호화한 후에는 파일명에 '.CRYPT' 확장자를 추가한다.



[그림] DearCry 로 암호화된 파일

[이미지 출처] https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

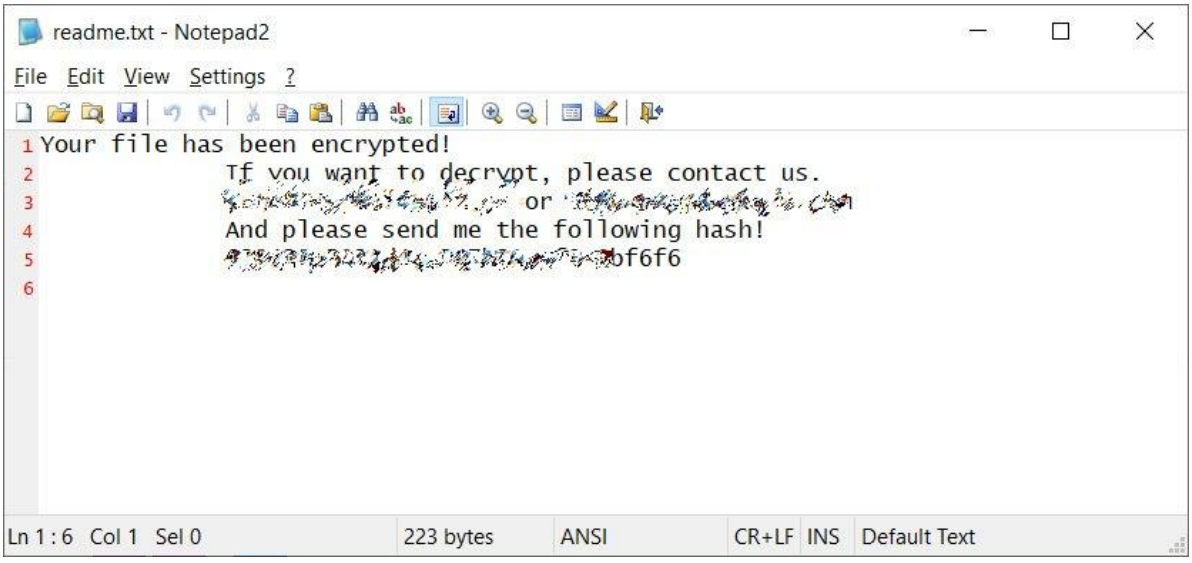
Gillespie 는 이 랜섬웨어가 파일 암호화를 위해 AES-256 및 RSA-2048 알고리즘을 사용하며, 암호화된 각 파일의 시작 부분에 'DEARCRY!' 문자열을 추가한다고 밝혔다.



[그림] 암호화된 파일 내 DEARCRY 파일 마커

[이미지 출처] https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

컴퓨터 암호화 작업이 끝나면 이 랜섬웨어는 데스크톱에 랜섬노트인 'readme.txt' 파일을 생성한다.
이 랜섬노트는 공격자의 이메일 주소 2 개와 고유 해시를 포함하고 있다. 연구원은 이 해시가 RSA 공개키의 MD4 해시라 밝혔다.



[그림] DearCry 랜섬노트

[이미지 출처] https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

안타깝게도 현재 이 랜섬웨어에는 파일을 무료로 복구할 수 있는 복호화 툴을 만들 수 있는 취약점이 없는 것으로 보인다.

- ProxyLogon 취약점 패치 필요해

DearCry 가 마이크로소프트 익스체인지 ProxyLogon 취약점을 통해 설치된다고 100% 확신할 수는 없지만, 현재 사용이 가능한 취약점을 활용할 가능성이 높다. Palo Alto Networks 에 따르면 최신 업데이트를 적용할 수 없는 구버전 서버가 여전히 약 8 만 대나 존재하는 것으로 나타났다. 전문가들은 모든 조직에서 가능한 빠른 시일 내 패치를 적용할 것을 권고했다.

[출처]

https://www.bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

https://twitter.com/phillip_misner/status/1370197696280027136

시스템 업데이트로 위장해 사용자를 스파잉하는 새로운 안드로이드 악성코드 발견

First New Android malware spies on you while posing as a System Update

감염된 안드로이드 기기에서 데이터를 훔치는 광범위한 스파이웨어 기능을 갖춘 새로운 악성코드가 발견되었다. 이 악성코드는 새로운 정보를 읽을 경우 유출을 위해 자동으로 트리거되도록 설계되었다. 이 스파이웨어는 타사 안드로이드 앱 스토어에서 '시스템 업데이트' 앱으로 설치되며, 구글의 공식 플레이스토어에는 등록되지 않았다.

- 악성코드, 거의 모든 정보 훔쳐

이 RAT 은 광범위한 정보를 수집하여 명령 및 제어 서버로 유출하는 기능을 포함하고 있었다. 이를 발견한 Zimperium 의 연구원들은 해당 악성코드가 "데이터, 메시지, 이미지를 훔치고 안드로이드 기기를 제어하는 것"을 관찰했다고 밝혔다. 해커들은 기기의 제어 권한을 얻게 되면 오디오 및 전화를 녹음하고, 사진을 찍고, 브라우저 히스토리를 확인하고, 왓츠앱 메시지에 접근하는 등의 행동을 수행할 수 있다. Zimperium 은 해당 데이터 탈취 기능이 다음을 포함하고 있다고 밝혔다.

- 인스턴트 메신저의 메시지 탈취
- 인스턴트 메신저의 데이터베이스 파일 탈취(루트 권한을 얻었을 경우)
- 기본 브라우저의 북마크와 검색 기록 검사
- 구글 크롬, 모질라 파이어폭스, 삼성 인터넷 브라우저의 북마크 및 검색 기록 검사
- .pdf, .doc, .docx, and .xls, .xlsx 를 포함한 특정 확장자 파일 탐색
- 클립보드 데이터 검사
- 공지 내용 검사
- 오디오 녹음
- 전화 통화 녹음
- 주기적으로 사진 촬영 (전면 또는 후면 카메라 사용)
- 설치된 애플리케이션 목록 열람
- 이미지 및 영상 탈취
- GPS 위치 모니터링

- SMS 메시지 탈취
- 전화 연락처 탈취
- 통화 기록 탈취
- 기기 정보 유출 (설치된 앱 목록, 기기 명, 저장소 통계 등)

이 악성코드가 안드로이드 기기에 설치되면, Firebase 명령 및 제어(C2) 서버로 저장소 통계, 인터넷 연결 타입, 왓츠앱 등 다양한 앱의 존재 여부 확인 등을 포함한 여러 조각으로 이루어진 정보를 보낸다. 이 스파이웨어는 루트 액세스 권한이 있는 경우 데이터를 직접 수집하고, 그렇지 않을 경우 사용자가 해킹된 기기에서 접근성 서비스를 활성화하도록 속인 후 이를 활용한다. 또한 외부 저장소에 저장되었거나 캐시된 데이터가 있는지 확인 후 수집하여 사용자가 Wi-Fi 를 연결할 때 C2 서버로 이를 전송한다.

- 잘 보이는 곳에 숨겨

데이터를 훔치도록 설계된 다른 악성코드와는 달리, 이 악성코드는 새로운 연락처 추가, 새로운 텍스트 메시지 수신, 새로운 앱 설치 등 일부 조건이 성립할 경우에만 안드로이드의 contentObserver 및 Broadcast 리시버를 통해 트리거된다. Zimperium 은 다음과 같이 언급했다. "Firebase 메시징 서비스를 통해 수신된 명령은 마이크를 통한 오디오 녹음, SMS 메시지 등의 데이터 유출과 같은 작업을 시작한다. Firebase 통신은 명령을 발행하는데만 사용되며, POST 요청을 통해 훔친 데이터를 수집하는데는 전용 C2 서버가 사용된다. 이 악성코드는 악성 행위를 숨기기 위해 마스터로부터 새로운 명령어를 수신할 경우 가짜 시스템 알림인 “업데이트 찾는 중” 메시지를 표기한다."

[그림] 가짜 시스템 업데이트 경고

[이미지 출처] https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/

또한 이 스파이웨어는 서랍/메뉴에서 아이콘을 숨겨 감염된 안드로이드 기기에서 자신의 존재를 숨긴다. 이는 탐지를 회피하기 위해 발견한 영상 및 이미지의 썸네일만 훔치므로 피해자의 대역폭 소비를 줄여 백그라운드에

서 이루어지는 데이터 유출 활동이 발각되지 않도록 한다. 대량으로 데이터를 수집하는 다른 악성코드와는 달리, 이 악성코드는 가장 최근 데이터만 추출한다. 이는 지난 몇 분간의 위치 데이터 및 활영된 사진만을 수집하는 것으로 나타났다.

[출처]

https://www.bleepingcomputer.com/news/security/new-android-malware-spies-on-you-while-posing-as-a-system-update/

https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/

(주)이스트시큐리티

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