이스트시큐리티

보안 동향 보고서

No.142 2021.07

No.142 2021.07

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

2021 년 6 월에는 세계적으로 랜섬웨어의 공격으로 인해 크고 작은 피해가 많이 발생하였습니다.

국내에서는 국내 기업들의 해외법인, 국내 성형외과, 산부인과, 피부과 등 병원에서 랜섬웨어의 공격으로 기밀정보 및 환자들의 민감정보들이 유출되었으며, 유출된 정보들 중 일부는 이미 딥 웹에 공개된 것으로 확인되었습니다. 해외의 경우 후지필름, ADATA 기업이 랜섬웨어의 공격을 받아 데이터가 유출되었습니다.

랜섬웨어의 공격과는 별개로 대량의 데이터 유출 사건도 발생하였습니다.

매출 기준 세계 최대 규모인 맥도널드의 미국, 한국, 대만 고객 및 직원의 데이터가 유출되었으며, 폭스바겐 역시 330 만 이상의 고객 개인정보가 유출되었다고 밝혔습니다. 미국의 슈퍼마켓 체인 Wegmans, LinkedIn 에서도 대규모의 데이터가 유출된 것으로 확인되어 정보가 유출된 사용자들의 이차 피해가 예상됩니다.

5 월부터 발생한 국내 기업을 타겟으로 한 북한의 해킹 그룹 Kimsuky 조직의 해킹 공격이 6 월에도 지속되었습니다. 지난 5 월, 대우조선해양과 원자력연구원(KAERI)을 대상으로 발생한 APT 공격 배후에 북한의 해킹 그룹 Kimsuky 가 연관되어 있는 것으로 밝혀졌습니다. 한국형 전투기(KF-21) 보라매를 생산하는 한국항공우주산업(KAI)도 해킹을 당했는데, Kimsuky 조직으로 추정되고 있어 국정원에서 특별 점검 중에 있습니다.

만약 이번 해킹공격을 통해 KF-21 과 3000t 급 잠수함의 자료가 실제로 유출되었다면 한국군 전력화에 큰 차질을 빚을 것으로 예상됩니다.

기업을 타겟으로 하는 공격이 끊임없이 발생하는 하고, 유출된 정보를 악용한 2 차 피해가 예상되는 만큼 기업 보안담당자들은 모니터링을 강화해야 합니다. 또한 해킹 공격 중의 상당부분이 임직원들의 부주의로 발생하는 만큼, 임직원들 보안의식 향상을 위한 주기적인 보안 교육이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021 년 6 월의 감염 악성코드 Top 15 리스트에서는 지난 몇 달간 1 위를 차지했던 Hosts.media.opencandy.com 이 2 위로 순위가 하락했으며 새롭게 탐지된 Heur.BZC.ONG.Pantera.14.C76F5E25 가 1 위를 차지했다. 이번 달에는 전체적으로 큰 순위 변동은 없었으나 Trojan.GenericFCA.Agent.7232 를 비롯한 8 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 그 외에 눈에 띄는 부분으로는 Misc.HackTool.KMSActivator 가 지난달 순위에서 6 계단 하락하여 14 위를 차지했다.

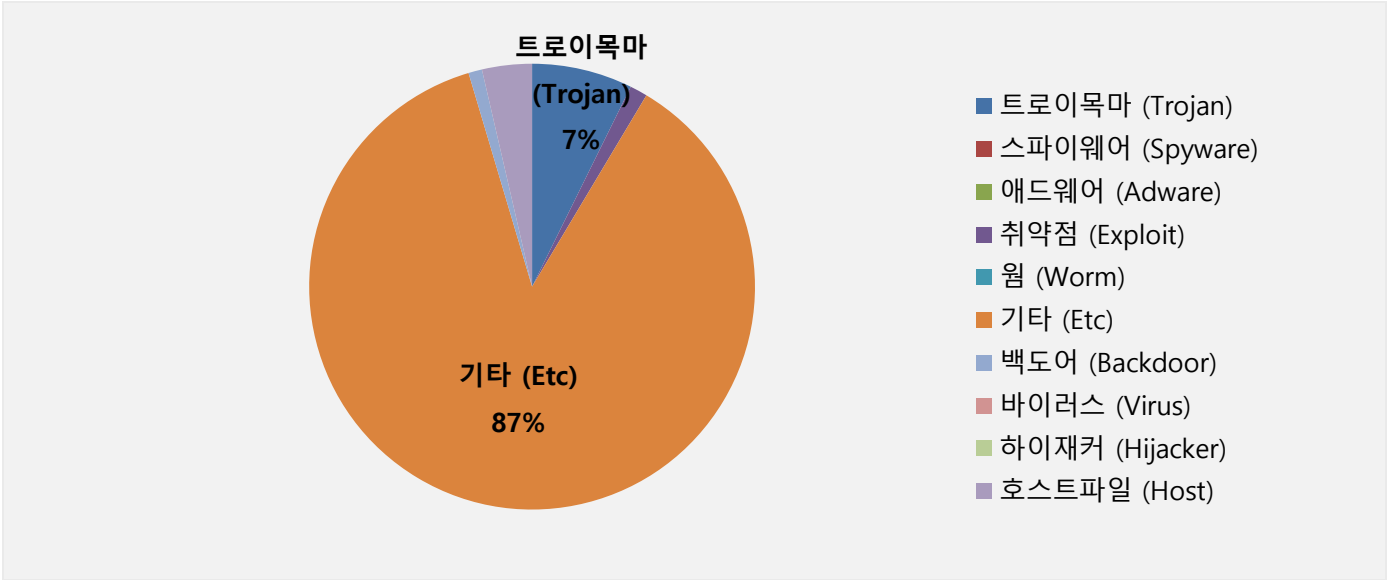
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	New	Heur.BZC.ONG.Pantera.14.C76F5E25	ETC	11,915,272
2	↓1	Hosts.media.opencandy.com	Host	556,971
3	New	Trojan.GenericFCA.Agent.7232	Trojan	530,117
4	↓2	Misc.Riskware.BitCoinMiner		ETC
5	↓1	Misc.HackTool.AutoKMS	ETC	310,661
6	↓1	Trojan.ShadowBrokers.A	Trojan	220,546
7	New	Exploit.CVE-2010-2568.Gen	Exploit	196,620
8	New	Trojan.Agent.FHCC	Trojan	194,966
9	↓3	Trojan.Agent.Injector.Gen	Trojan	178,945
10	New	Heur.BZC.YAX.Linx.15.05E78B67	ETC	168,646
11	New	Gen:Variant.Zusy.319562	ETC	159,527
12	↓5	Backdoor.Generic.792814	Backdoor	152,104
13	New	Gen:Variant.Razy.767621	ETC	134,589
14	↓6	Misc.HackTool.KMSActivator	ETC	126,383
15	New	Gen:Variant.Application.Keygen.16	ETC	124,111

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 06 월 01 일 ~ 2021 년 06 월 30 일

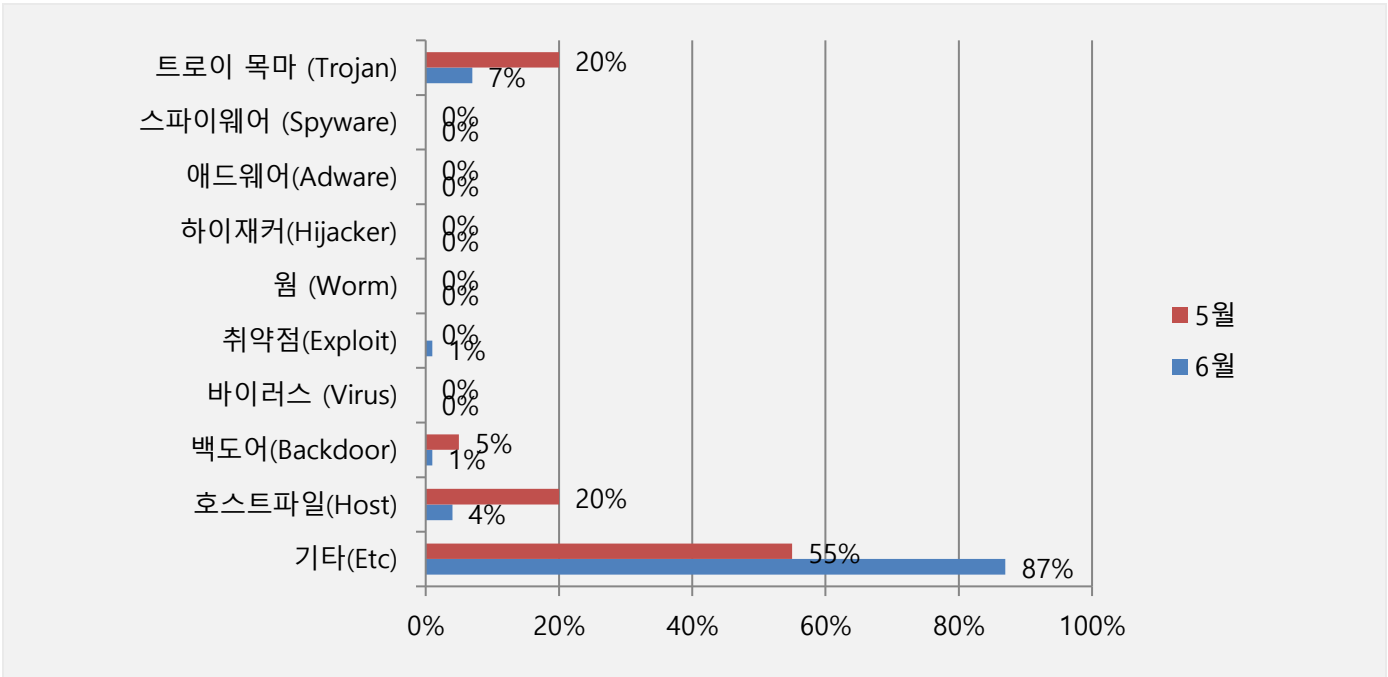
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 87%를 차지했으며 트로이목마(Trojan) 유형과 호스트 파일(Host) 유형이 각각 7%와 4%로 그 뒤를 이었다. 지난달 5%를 차지했던 백도어(Backdoor) 악성코드 유형은 대폭 감소하여 1%를 기록했다. 2021 년 5 월과 비교하여 전체 감염 건수는 약 377.55% 증가하였다.



카테고리별 악성코드 비율 전월 비교

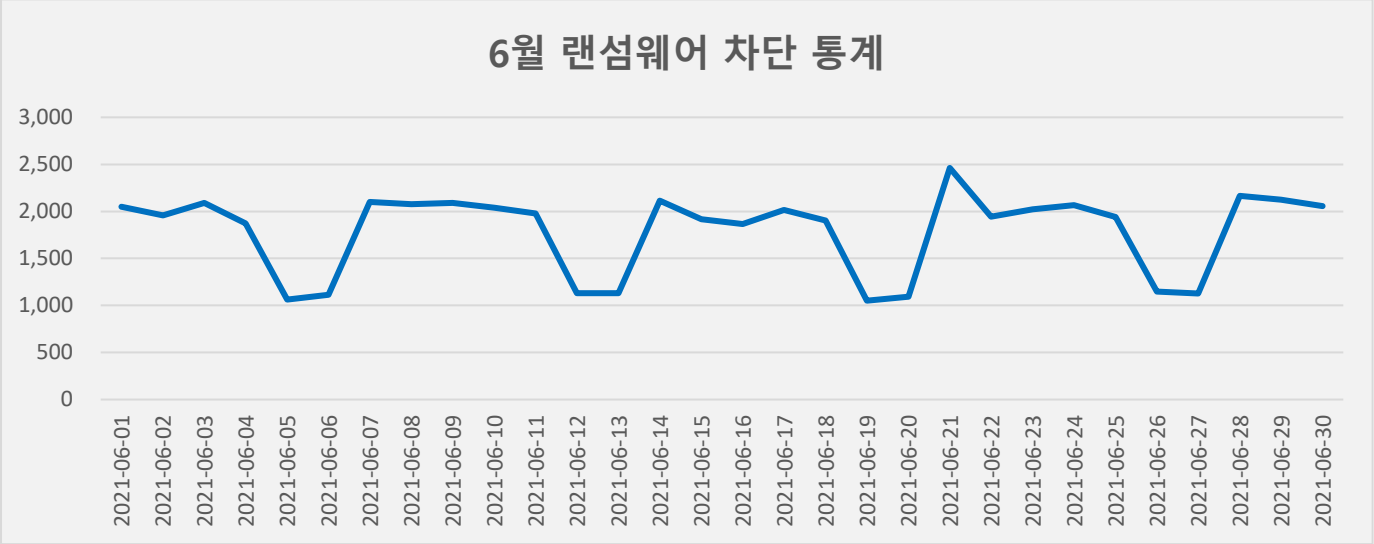
6 월에는 지난 5 월과 비교하여 트로이목마(Trojan) 유형이 13% 감소하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 16% 감소했다. 5 월에 5%를 차지했던 백도어(Backdoor) 유형이 대폭 감소하여 1%를 기록했다. 이는 6 월 한 달간 ETC 유형의 Heur.BZC.ONG.Pantera.14.C76F5E25 악성코드가 다량 탐지되어 ETC 유형이 87%를 기록한 영향으로 보인다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

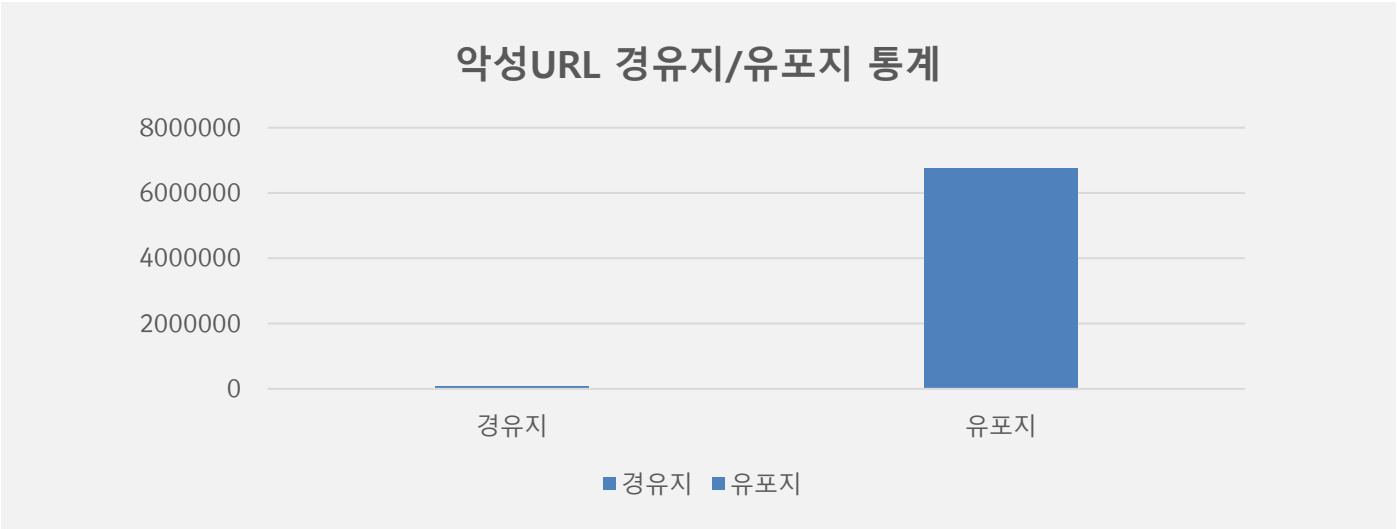
6 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 6 월 1 일부터 6 월 30 일까지 총 53,704 건의 랜섬웨어 공격 시도가 차단되었다. 5 월의 랜섬웨어 공격 건수인 51,742 건에 비해 약 3.79% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 6 월 한 달간 총 6,822,860 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 5 월 한 달간 확인되었던 6,976,796 건의 악성코드 경유지/유포지 URL 수에 비해 약 2.21% 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 2 분기 랜섬웨어 행위기반 차단 건수: 158,188 건!

2. Babuk 랜섬웨어 Builder 분석

1. 알약 2 분기 랜섬웨어 행위기반 차단 건수: 158,188 건!

2021 년 2 분기, 알약을 통해 총 158,188 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 탐지 건까지 포함한다면 전체 공격은 더욱 많을 것으로 예상됩니다.

통계에 따르면, 2021 년 2 분기 알약을 통해 차단된 랜섬웨어 공격은 총 158,188 건으로, 이를 일간 기준으로 환산하면 일 평균 약 1,758 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다. 최근 2 년에 걸쳐 전체 랜섬웨어 공격 건수는 지속적으로 감소하는 추세를 보였으나, 지난 1 분기에 비해 2 분기부터는 조금씩 증가하는 모습을 보이고 있습니다.

[그림] 알약 랜섬웨어 행위기반 차단 기능'을 통해 차단된 2021 년 2 분기 랜섬웨어 공격 통계

02 전문가 기고

ESRC 는 2021 년 2 분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

1) Sodinokibi 조직의 전방위적 공격 확산 및 새로운 리눅스 변종 발견
2) 미 최대 송유관 회사 Colonial Pipeline 등 국가 인프라 타깃 대규모 공격 발생
3) Babuk Locker 랜섬웨어 빌더 유출로 변종 및 실제 피해 사례 다수 발생
4) '비너스락커' 그룹이 유포하는 Makop 랜섬웨어 공격 꾸준히 발생

2021 년 2 분기에는 피싱 이메일 내 입사 지원서, 저작권 침해 관련, 견적 문의 등 다양한 테마의 첨부파일 형태로 유포되는 Makop 랜섬웨어가 꾸준히 상위권을 유지했습니다. 전 세계 유명 기업들을 타깃으로 다수의 공격을 펼치며 새로운 리눅스 변종까지 제작한 Sodinokibi 랜섬웨어 그룹의 움직임도 주목할 만합니다. 미국 송유관 시설을 타깃으로 수행된 Darkside 랜섬웨어 공격으로 인해 막대한 피해가 발생했으며, 그 밖에 Babuk Locker 랜섬웨어의 빌더 유출로 변종 제작 및 실제 악용 사례가 확인되었습니다. 2 분기 랜섬웨어 공격 건수는 1 분기에 비해 전반적으로 증가 추세를 나타냈습니다.

2 분기에 주목할만한 위협으로는 4 월에 발생한 Apple 의 핵심 공급업체인 대만의 'Quanta Computer' 공격, 6 월에 발생한 미국 식품 가공 업체 'JBS Food' 및 일본 기업 'Fujifilm' 공격 등 세계적인 대기업을 대상으로 Sodinokibi (Revil 로도 알려짐) 그룹 소행으로 의심되는 랜섬웨어 공격들이 잇따라 발생했습니다. 이로 인해 여러 생산 시설들이 일정 시간 중단되는 등 시스템 운영에 어려움을 겪었으며, 해커들은 탈취한 데이터 중 핵심적인 기업 기밀 사항 등을 유출하겠다고 협박하는 '이중 갈취' 전략을 사용함으로써 랜섬 지불을 더욱 효과적으로 유도했습니다. 6 월 말에는 VM 웨어 ESXi 를 공격하는 Sodinokibi 랜섬웨어의 리눅스 변종이 발견되었습니다. 리눅스 아키텍처에 Windows 버전을 추가하는 Sodinokibi 업그레이드 방식은 Darkside 와 같은 인기 있는 RaaS 그룹에서 최근 자주 활용되는 추세로, 잠재적 공격 타깃 범위를 확장하는 데 효과적입니다.

5 월에는 미국 최대 송유관 기업인 'Colonial Pipeline' 시설을 노린 Darkside 랜섬웨어 공격이 발생했습니다. 해당 공격으로 인해 5 일 간 미 전역에 공급되는 5,500 마일 길이의 파이프라인 운영이 5 일간 중단되었고, 5 백만 달러에 달하는 거액의 랜섬 머니를 지불한 뒤 비로소 운영을 재개했습니다. 해당 기업은 제품 공급 중단으로 인해 가스 가격이 상승하는 등 전 세계 경제 상황에 심각한 피해를 초래할 것으로 예상되어, 비용을 지불하고 도난당한 데이터 유출을 막은 것으로 확인되었습니다. 공격 발생 이후, FBI 공조 등을 통해 대대적인 수사가 이루어졌고, 결국 Darkside 랜섬웨어 운영자들은 폐업을 선언하고 피해 기업에 복호화 키를 제공하겠다고 밝혔습니다. 'Colonial Pipleline' 공격은 에너지 산업의 핵심 인프라에 대한 공격이 매우 위험할 수 있음을 다시 한번 보여주는 사례로 평가됩니다.

4 월에는 Babuk Locker 랜섬웨어 조직이 미국 워싱턴 DC 경찰국에서 데이터 탈취를 주장하며 금전 지불을 요구했고, 지불이 이루어지지 않을 경우 기밀 정보들을 추가로 공개하겠다고 피해자들을 협박했습니다. 6 월에는 Babuk Locker 랜섬웨어의 빌더가 VirusTotal 악성코드 스캐닝 서비스에 등록되었으며, 보안 연구원에 의해 발견되었습니다. 해당 빌더 유출로 인해 다른 사이버 범죄 조직이 자체 버전을 개발함으로써 전 세계의 조직을 공격할 수 있기 때문에 더욱 우려되는 상황으로 Babuk Locker 랜섬웨어 공격과 관련된 지속적인 모니터링이 필요합니다.

02 전문가 기고

지난 1 분기에 이어 2 분기에도 비너스락커 그룹이 유포하는 Makop 랜섬웨어가 꾸준히 발견되었습니다. Makop 공격자들은 주로 입사지원서, 이력서, 경력 사항, 포트폴리오, 견적 문의 또는 이미지 저작권 침해 관련 문서로 위장한 EXE 파일을 첨부한 스피어피싱 이메일 형태로 랜섬웨어를 유포했습니다. 특히 파일 아이콘, 파일명, 파일 설명, 확장명, 메일 주소 등은 다양하게 변경해가며 탐지 망을 교묘히 피해 가는 수법을 이용했고, 그 외 특징들은 이전과 유사합니다.

이밖에도 Sodinokibi 와 랜섬노트 웹페이지 디자인이 동일한 새로운 'Lorenz' 랜섬웨어와 Sodinokibi 소스코드를 기반으로 제작된 'LV' 랜섬웨어가 발견되었습니다. Lorenz 랜섬웨어는 커스텀 공격을 통해 전 세계 기업을 노리며 4 월부터 활동을 시작했습니다. 다른 랜섬웨어 그룹과는 약간 다른 방식으로 데이터를 게시하는데, 랜섬 지불을 압박하기 위해 다른 공격자 또는 경쟁 업체에 데이터 판매를 허용하고 피해자 내부 네트워크 접근 권한도 함께 판매합니다. LV 랜섬웨어는 Sodinokibi 바이너리를 복사하고 용도를 변경함으로써 자체 랜섬웨어를 제작한 것으로 확인되며, 데이터를 탈취하고 "name and shame" 유출 사이트에 피해자 이름을 게시하는 등 다양한 방법으로 Sodinokibi 랜섬웨어의 공격 방식을 모방하였으나 명확하게 구별되는 차이점들도 존재해, 독자적으로 개발된 랜섬웨어로 확인되었습니다. LV 랜섬웨어는 해커들이 이미 공격 성공률이 검증된 잘 알려진 랜섬웨어 코드를 활용함으로써 개발 리소스를 절감하고 수익성 높은 비즈니스 모델을 구축할 수 있음을 잘 보여주는 사례입니다.

그 외, QLocker, Avaddon, Darkside 등 일부 랜섬웨어 그룹들이 운영 중단을 선언하고 피해자의 복호화 키를 공개하거나 공개 예정이라고 밝혔습니다. QLocker 랜섬웨어의 경우 FBI 로 위장한 익명 제보를 통해 복호화 키가 전달되었고 조사 결과 실제 복호화 키로 확인되었습니다. 각각의 키는 특정 피해자들에게 할당되었습니다. 4 월부터 수백만 명의 QNAP 사용자를 공격한 QLocker 랜섬웨어 또한 운영을 중단한다고 발표했습니다. 이들이 랜섬을 탈취하기 위해 사용했던 QLocker Tor 사이트가 모두 접근 불가 상태로 확인되었습니다. Darkside 랜섬웨어 운영자들 또한 FBI 공조 수사가 진행되자 활동을 중단한다고 밝혔습니다. 이들은 최근 주요 인프라에 대한 공격 이후 전 세계 법 집행 기관 및 정부의 압력에 따라 이 같은 결정을 한 것으로 추정됩니다.

이스트시큐리티 ESRC 이지현 팀장은 "2021 년 2 분기에도 Makop 랜섬웨어를 활용한 비너스락커 그룹의 공격이 지속적으로 발견되고 있다."라고 언급하며, "최근에는 해커들이 기존에 잘 알려진 랜섬웨어의 소스코드나 공격 방식을 활용함으로써 공격 효율성을 높이고 있으며, 국가 핵심 인프라 시설 및 유통 기업을 대상으로 하는 대규모 공격들도 과감하게 이루어지고 있어, 추후 심각한 피해로 이어지는 것을 예방하기 위해서는 기업과 개인들은 주기적인 백업 및 안전한 보안 시스템 구축 등을 통해 사전에 대비하는 자세가 필요하다."고 강조했습니다.

이밖에 ESRC 에서 밝힌 2021 년 2 분기에 새로 발견되었거나, 주목할만한 랜섬웨어는 다음과 같습니다.

랜섬웨어 명	주요 내용
FiveHands	DeathRansom(HELLOKITTY) 변종 랜섬웨어로, UNC2447 사이버 범죄 조직이 SonicWall VPN 제로데이(0-Day) 취약점을 이용하여 유럽, 북미 지역을 대상으로 SombRAT 악성코드 감염을 시킨 후 유포됨.

Nitro	디스코드(Discord) Nitro 선물 코드를 랜섬머니로 요구하는 랜섬웨어로, 암호화된 파일에 '.giveme nitro' 확장자를 추가함. 또한 피해자 바탕화면을 화난 표정을 지은 디스코드(Discord) 로고로 변경하며, 피해자가 유효한 선물코드 링크 입력시 파일을 복호화함.
Epsilon Red	Microsoft Exchange 서버의 패치되지 않은 취약점 'ProxyLogon' 을 악용하는 랜섬웨어로, 암호화된 파일에 확장자 '.epsilonred'를 추가함. Golang(Go) 언어로 작성되었으며, Sodinokibi 랜섬웨어의 랜섬노트를 일부 모방하여 사용함.
Marketo	일본의 중장비 업체 '고마쓰(KOMATSU)'를 해킹했다고 밝히며, 산업기밀 및 개인정보를 경쟁사에 유출했다는 내용으로 피해자의 랜섬 지불을 압박한 랜섬웨어로, 이중 갈취 수법에서 한 단계 진화한 형태로 제작됨. 세계적인 중장비 업체들의 이메일 주소를 함께 공개해 주장의 신뢰성을 높임.
Cring	패치되지 않은 Fortinet VPN 기기를 공격한 랜섬웨어로, CVE-2018-13379 취약점을 적극적으로 악용함. 파일 암호화 후 최대 2BTC 를 랜섬으로 요구하며, Cobalt Strike 프레임워크를 사용해 랜섬웨어를 배포함.
N3TW0RM	이스라엘에 위치한 기업 및 비영리단체를 타깃으로 공격을 수행한 랜섬웨어로, 파일 암호화 및 데이터 유출 협박을 동시에 진행하는 '이중 갈취' 전략을 사용함. 클라이언트-서버 모델을 사용하여 공격을 수행하며, 암호화된 파일에는 '.n3tworm' 확장자가 추가됨.
DarkRadiation	Linux 와 Docker 클라우드 컨테이너를 타깃으로 하며 Bash 셸로 작성된 랜섬웨어로, 암호화된 파일의 이름에 방사능 기호를 추가함. 복잡한 Bash 스크립트 모음과 최소 6 개의 C2 를 사용하며, 하드코딩된 API 키를 사용해 Telegram 봇과 통신하는 것이 특징.
Cuba	암호화된 파일 내부에 피델 카스트로(Fidel Castro)를 지칭하는 문구가 포함된 랜섬웨어로, 카리브 제도에 위치한 쿠바(Cuba) 국가를 연상시키는 파일 확장명이 포함됨. 북미, 남미, 유럽 전역의 금융 기관, 기술, 물류 산업을 타깃으로 공격을 수행함.

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. Babuk 랜섬웨어 Builder 분석

2021 년 1 월 최초로 등장한 Babuk 랜섬웨어는 지난 4 월까지 전 세계 기업 및 특정 개인을 대상으로 활발한 공격 활동을 펼쳤습니다.

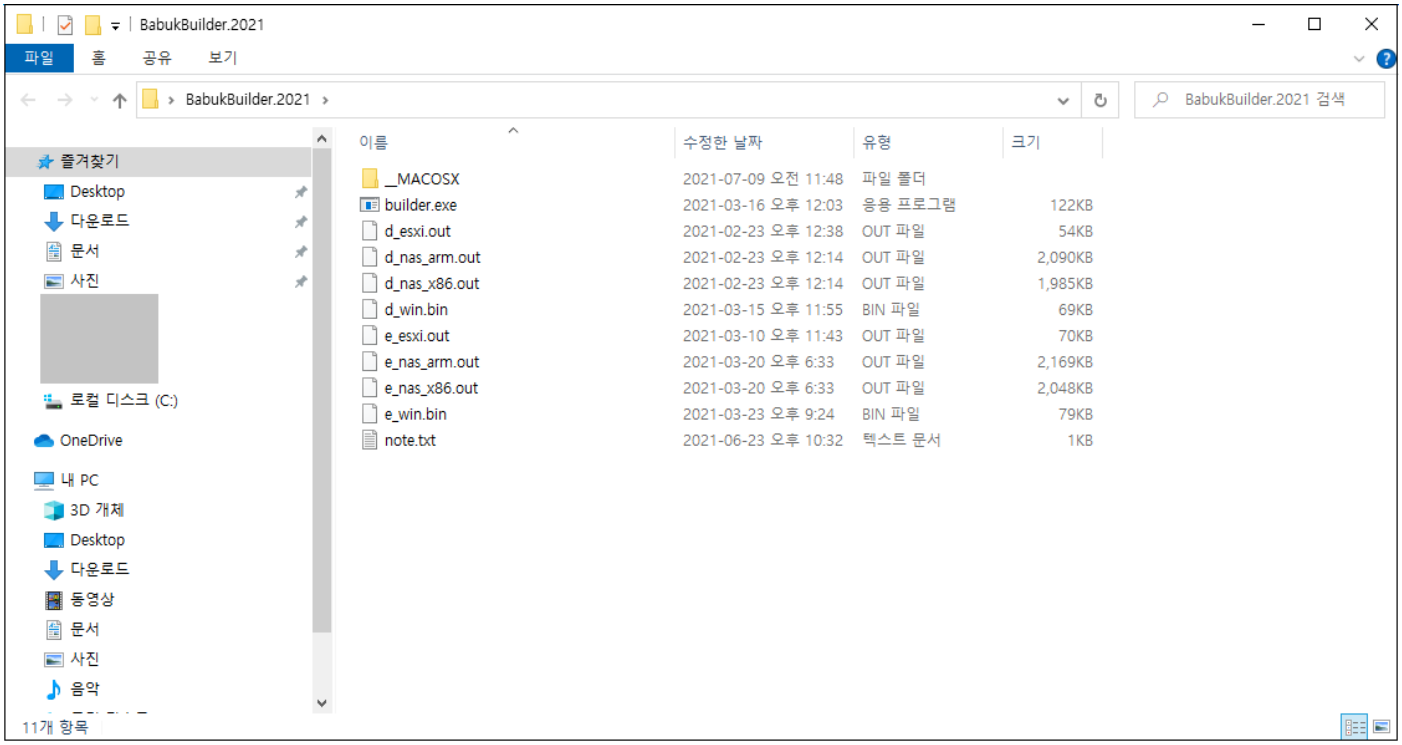
하지만 지난 4 월, 워싱턴 DC 경찰서 공격을 마지막으로 랜섬웨어 운영을 중단하였습니다.

그 후 5 월 말, Babuk 랜섬웨어 운영자는 데이터 유출 사이트를 Payload.bin 으로 리브랜딩 후 다른 공격자들에게 피해자들로부터 훔친 데이터를 유출할 수 있는 기회를 제공하였습니다.

6 월 말, 악성코드 스캐닝 사이트 Virustotal 에 Babuk 랜섬웨어 빌더가 업로드되었으며, 이를 한 보안 연구원이 발견하였습니다. 이 빌더가 Virustotal 사이트에 업로드된 경위는 아직 확인되지 않았습니다.

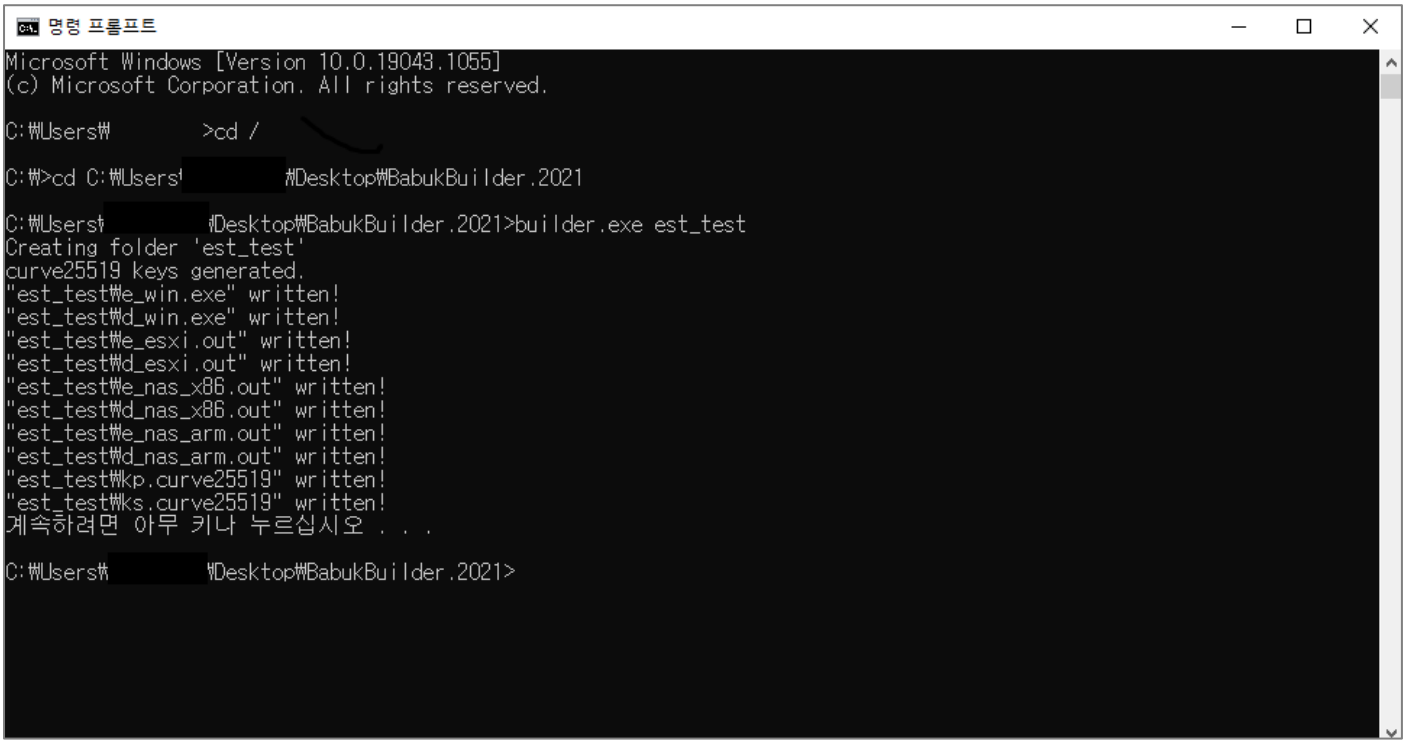
이에 ESRC 에서는 해당 Babuk 랜섬웨어 Builder 에 대해 간단히 분석해 보았습니다.

Virustotal 에 올라온 Babuk 랜섬웨어 Builder 는 다음과 같은 파일로 구성되어 있습니다.



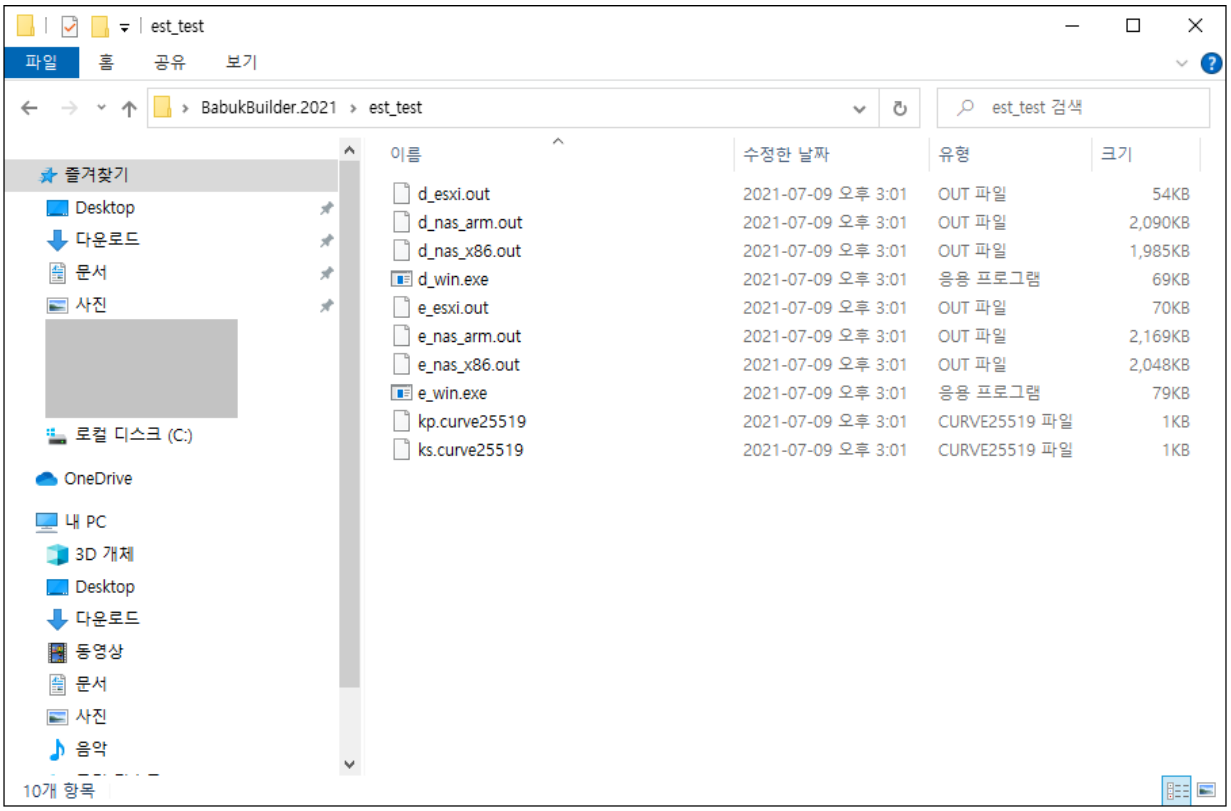
[그림 1] 압축 해제한 Babuk Ransomware builder

우리는 Builder.exe 파일을 실행하여 암호화/복호화 파일을 생성해보았습니다.



[그림 2] est_test 폴더 생성

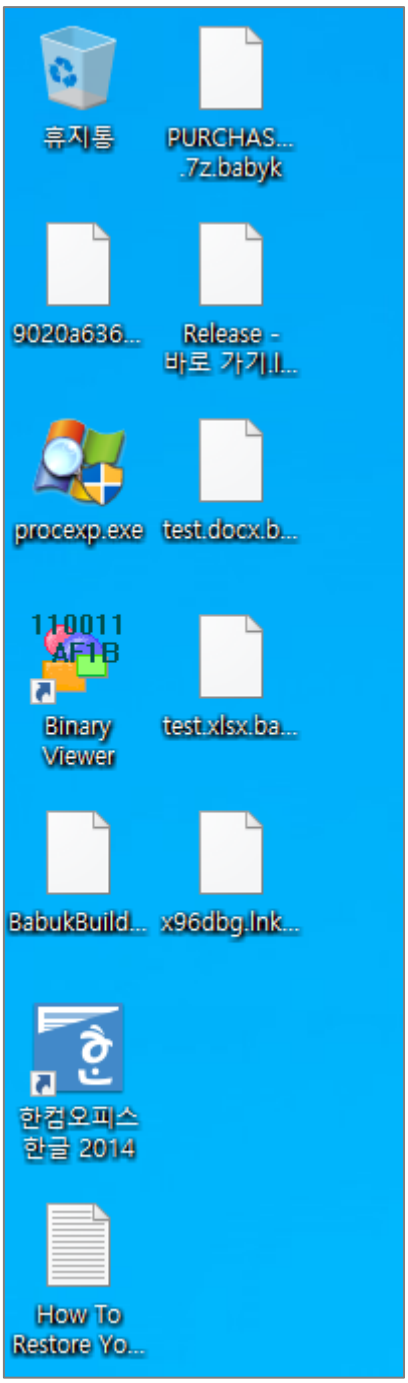
생성된 바이너리 파일들은 다음과 같습니다.



[그림 3] 생성된 est_test 폴더

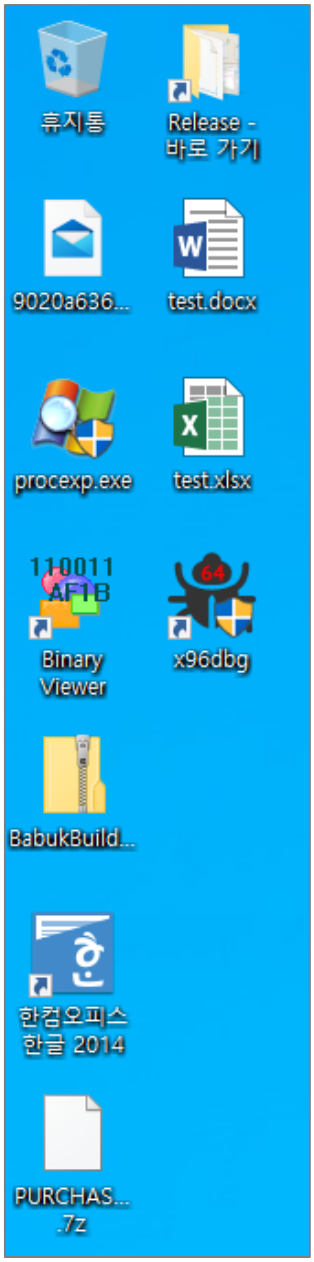
생성된 바이너리 파일들 중 e_win.exe 파일은 파일들을 암호화할 때 사용되며, d_win.exe 파일은 암호화된 파일들을 복호화할 때 사용합니다.

e_win.exe 파일을 실행하면, 다음과 같이 파일들을 .babyk 확장자 파일로 암호화를 하며 랜섬노트를 생성합니다.



[그림 4] 암호화된 화면

다시 d_win.exe 파일을 실행하면, 암호화된 파일들이 다시 복호화가 됩니다.



[그림 4] 복호화된 화면

암호화키와 랜섬노트는 하드코딩 되어있으며, 리버싱을 통해 해당 부분만 변경한다면 누구나 해당 빌더를 이용하여 손쉽게 랜섬웨어를 제작할 수 있습니다.

이번 랜섬웨어 빌더 유출로 인해 랜섬웨어 공격 증가가 예상되는 만큼, 사용자 및 기업들의 각별한 주의가 요구되고 있습니다.

현재 알약에서는 해당 랜섬웨어 빌더에 대해 Misc.Riskware.RansomBuilder, Trojan.Ransom.Babuk 로 탐지중에 있습니다.

03
악성코드 분석 보고

[Trojan.PSW.Ficker] 악성코드 분석 보고서

Trojan.PSW.Ficker(이하 'Ficker Stealer')는 MaaS(Malware as a Service)로 제공되는 정보 유출 악성코드로, 음원 관련 특정 애플리케이션의 사칭이나 Hancitor 다운로더 등에 의해 유포가 되는 것으로 알려져 있다. 이 악성코드는 감염 PC 정보와 웹 브라우저 등의 애플리케이션 크리덴셜 정보 탈취와 더불어 추가 페이로드 다운로드 실행 기능을 수행한다.

```
.text:00415848 010 8D 05 81 1E 43+          lea     eax, loc_431E81
.text:0041584E 010 B9 60 7F 43 00           mov     ecx, offset unk_437F60
.text:00415853 010 BA 23 FE FF FF           mov     edx, -1DDh
.text:00415858 010 89 03                    mov     [ebx], eax
.text:0041585A 010 B8 9B 38 FF FF           mov     eax, -0C765h    ; 0x431E81 - 0xc765 = 0x42571C
.text:0041585F 010 01 D1                    add     ecx, edx
.text:00415861 010 03 03                    add     eax, [ebx]
.text:00415863 010 51                       push    ecx
.text:00415864 014 57                       push    edi
.text:00415865 018 53                       push    ebx
.text:00415866 01C FF D0                    call    eax             ; DecryptString Function
.text:00415868 01C 83 C4 0C                 add     esp, 0Ch
.text:0041586B 010 53                       push    ebx             ; lpProcName
.text:0041586C 014 56                       push    esi             ; hModule
.text:0041586D 018 E8 0A F4 01 00           call    GetProcAddress
.text:00415872 010 89 C7                    mov     edi, eax
.text:00415874 010 8D 05 0D EF 42+          lea     eax, loc_42EF0D
.text:0041587A 010 B9 74 7F 43 00           mov     ecx, offset unk_437F74
.text:0041587F 010 BA 23 FE FF FF           mov     edx, -1DDh
.text:00415884 010 89 03                    mov     [ebx], eax
.text:00415886 010 B8 0F 68 FF FF           mov     eax, -97F1h     ; 0x42EF0D - 0x97F1 = 0x42571C
.text:0041588B 010 01 D1                    add     ecx, edx
.text:0041588D 010 03 03                    add     eax, [ebx]
.text:0041588F 010 51                       push    ecx
.text:00415890 014 6A 0D                    push    0Dh
.text:00415892 018 59                       pop     ecx
.text:00415893 014 51                       push    ecx
.text:00415894 018 53                       push    ebx
.text:00415895 01C FF D0                    call    eax
```

[그림] 함수 주소 난독화 코드 중 일부

Ficker Stealer'는 감염 PC 정보, 애플리케이션 크리덴셜 정보 탈취 기능과 추가 페이로드 다운로드 기능을 가진 악성코드이다. 로컬 정보를 확인하여 동구권 국가인 경우 프로그램 종료하는 점, 정보 탈취 목적과 더불어 추가 페이로드 기능이 있는 점이 특징적이다.

기업이나 개인이 이 악성코드에 감염이 되는 경우, 정보 유출과 더불어 지갑 정보 탈취에 의해 금전 피해를 입을 가능성이 높다.

따라서, 이 악성코드를 예방하기 위해서는 윈도우 보안 업데이트와 백신 제품의 업데이트를 항상 최신으로 유지, 출처가 불분명한 사이트에서 다운로드는 삼가는 보안 습관을 가져야 한다.

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

[Trojan.Android.Banker] 악성코드 분석 보고서

해외에서도 스미싱 공격이 유행이다. 최근에 발견된 Flubot 악성 앱도 문자메시지를 통해 전파되며 피해자의 금융 정보 탈취를 목적으로 제작된 악성 앱이다.

문자메시지는 Fedex 와 같은 택배 회사를 사칭하고 있으며 한국과 비슷하게 택배 수령 날짜 등의 정보를 확인이 필요하다는 내용으로 구성되어 있다. 피해자가 문자메시지의 내용에 속아 메시지 내의 링크를 클릭하면 악성 앱 설치를 유도하는 웹 페이지를 방문하게 되고 웹 페이지의 안내에 따라 악성 앱을 설치하게 되는 식이다.

[그림] 앱 실행 화면

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

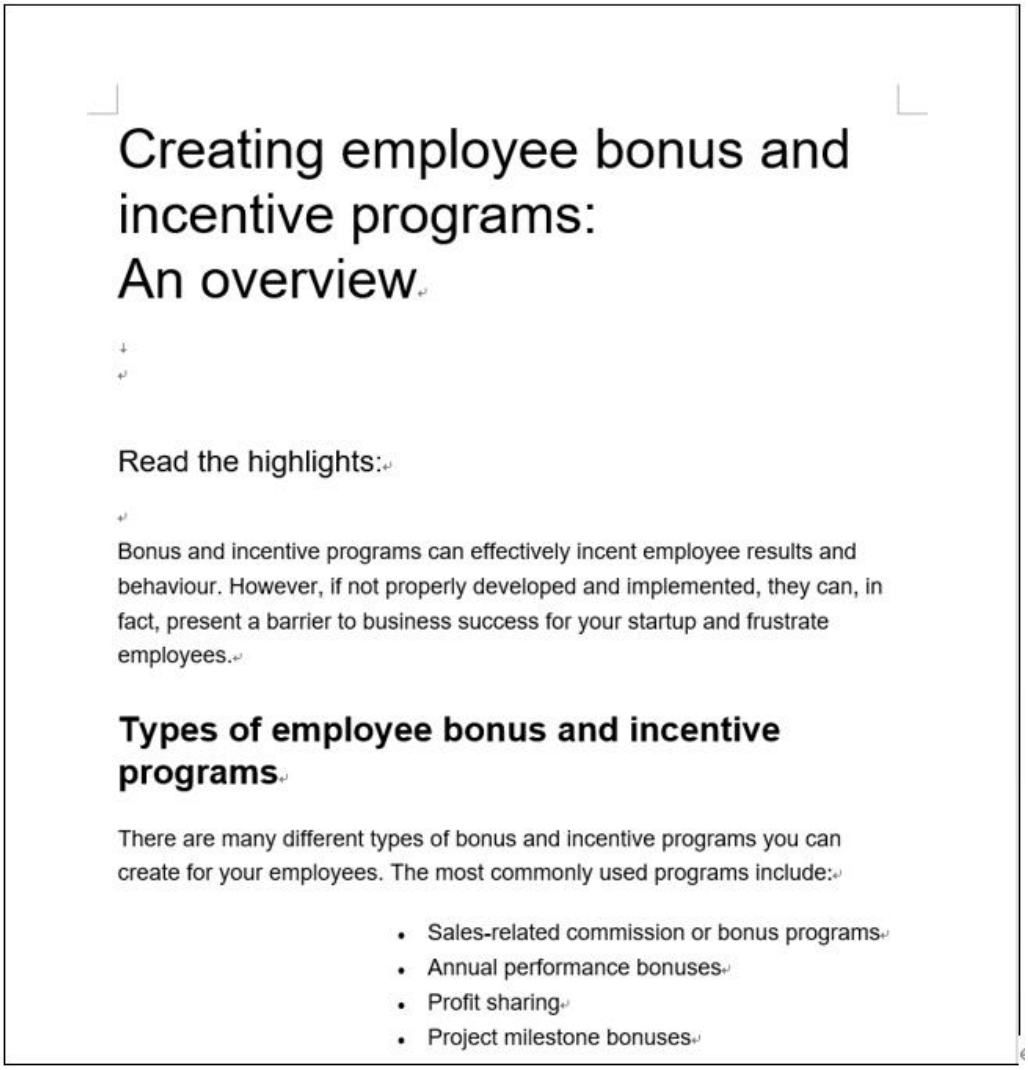
현재 알약 M 에서는 해당 앱을 ‘Trojan.Android.Banker’ 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

라자루스 APT 그룹, 중국 정부 및 기업 대상으로 피싱 공격 수행

瑞星预警：APT 组织 Lazarus Group 对中国发起攻击

중국의 Rising 그룹은 중국의 정부와 민간 기업에 대한 APT 공격을 포착하였다. 공격자가 공격에 성공하면 컴퓨터를 원격 제어하여 임의 코드를 실행하고 중요한 데이터와 정보를 훔친다. 보안 전문가들이 이번 공격에 대해 분석을 진행한 결과 이번 공격 배후에 라자루스 그룹(Group 77, Hastati Group, Hidden Cobra, APT-C-26, T-APT 그룹이라고도 알려짐)이 있는 것으로 밝혀졌다.



Creating employee bonus and incentive programs: An overview

Read the highlights:

Bonus and incentive programs can effectively incent employee results and behaviour. However, if not properly developed and implemented, they can, in fact, present a barrier to business success for your startup and frustrate employees.

Types of employee bonus and incentive programs

There are many different types of bonus and incentive programs you can create for your employees. The most commonly used programs include:

- Sales-related commission or bonus programs
- Annual performance bonuses
- Profit sharing
- Project milestone bonuses

[이미지 출처] http://it.rising.com.cn/dongtai/19777.html

공격 대상 국가로는 중국, 독일, 호주, 일본 등이 있으며, 타깃이 되는 산업 분야는 항공 우주, 정부, 의료, 금융, 미디어 등으로, 주로 직원 보너스 및 인센티브 계획 생성에 관한 내용의 악성 파일을 통해 공격을 진행한 것으로 밝혀졌다.

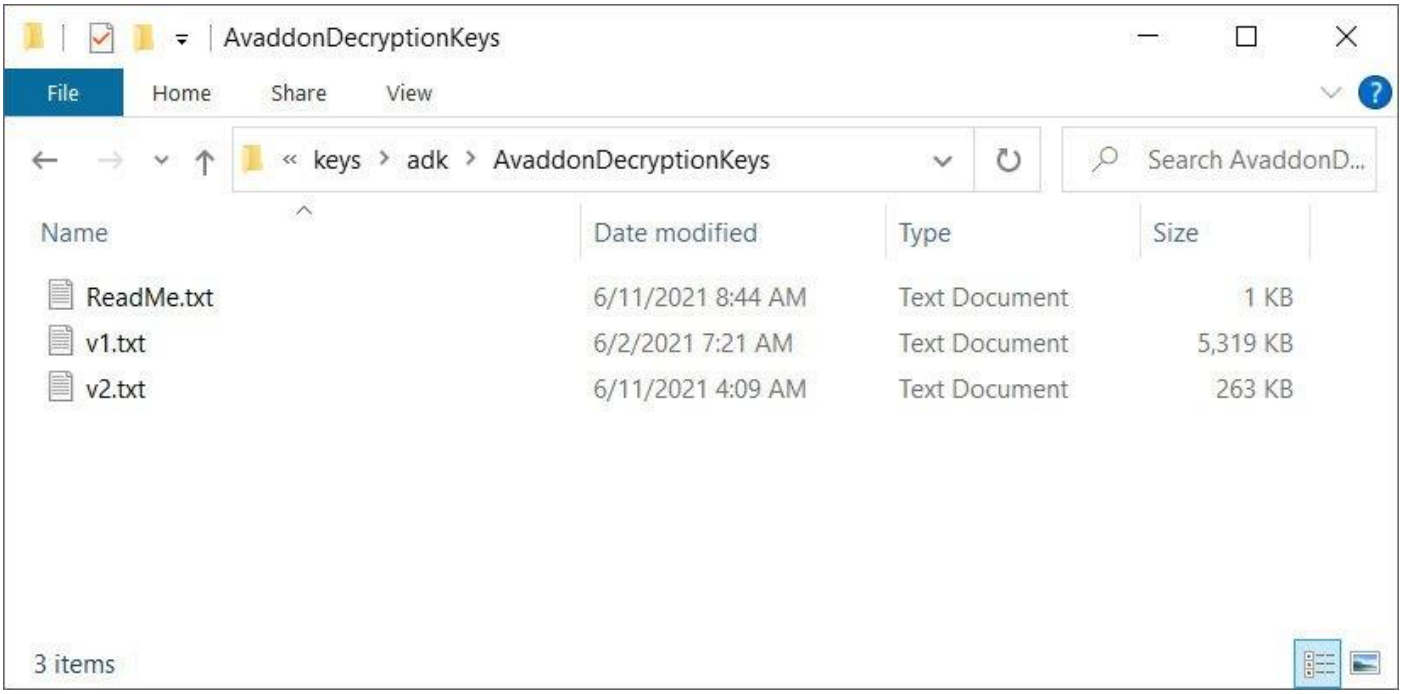
[출처]

http://it.rising.com.cn/dongtai/19777.html

Avaddon 랜섬웨어, 활동 중단 후 복호화 키 공개해

Avaddon ransomware shuts down and releases decryption keys

Avaddon 랜섬웨어 그룹이 운영을 중단하고 Bleeping Computer 측에 피해자의 복호화 키를 공개했다. 11 일 아침, Bleeping Computer 에서는 FBI 로 위장한 한 익명 제보를 받았다. 해당 제보에는 비밀번호로 보호된 ZIP 파일로 연결되는 링크와 비밀번호가 포함되어 있었다. 해당 파일은 "Avaddon 랜섬웨어의 복호화 키"라 되어있었으며 아래 파일 3 개를 포함하고 있었다.



[이미지] BleepingComputer 에 공유된 Avaddon 복호화 키

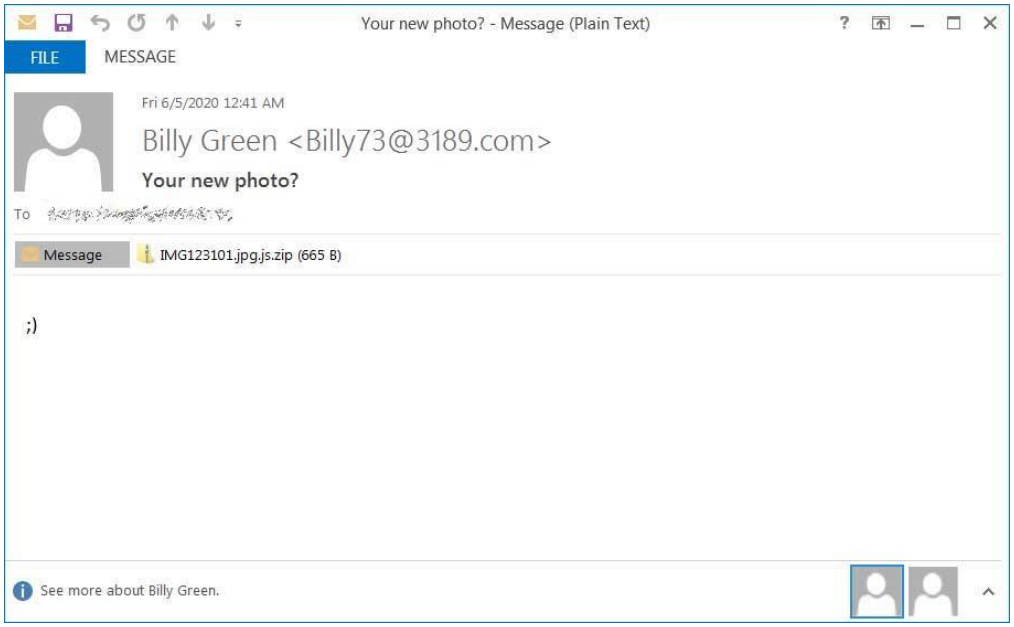
[이미지 출처] https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

여러 연구원들이 해당 파일을 확인한 결과 이 복호화 키는 진짜인 것으로 나타났다. BleepingComputer 는 Emsisoft 에서 공유한 테스트 복호화 툴을 통해 최근 Avaddon 샘플로 암호화된 가상 머신을 복호화하는 데 성공했다. 범죄자들은 복호화 키 총 2,934 개를 공유했으며, 각 키는 특정 피해자에 할당된다. Emsisoft 는 모든 피해자가 무료로 파일을 복구할 수 있는 무료 복호화 툴을 공개했다.

자주는 아니지만, 랜섬웨어 그룹은 운영을 종료하거나 새로운 버전을 출시할 때 여러 연구원에게 복호화 키를 공유하는 경우가 있었다. 과거에도 TeslaCrypt, Crysis, AES-NI, Shade, FilesLocker, Ziggy, FonixLocker 용 복호화 키가 공개된 바 있다.

Avaddon 랜섬웨어 운영 중단

Avaddon 랜섬웨어는 2020년 6월 활동을 시작해 다음의 윙크 이모티콘이 포함된 피싱 캠페인을 통해 확산되었다.



[이미지] Avaddon 피싱 이메일

[이미지 출처] https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

시간이 지남에 따라, Avaddon의 규모는 더욱 커져 FBI와 호주 법 집행부에서 최근 해당 그룹과 관련된 보안 권고를 발표하기에 이르렀다. 현재 Avaddon 의 모든 tor 사이트는 접근할 수 없는 상황이기 때문에, 랜섬웨어 운영이 종료되었을 가능성이 있다. 또한 랜섬웨어 협상 회사 및 사건 대응자들은 Avaddon 랜섬웨어가 최근 며칠 동안 랜섬머니를 지불하지 않은 피해자가 지불을 완료하도록 협박하는 것을 목격했다고 밝혔다. Coveware 의 CEO 인 Bill Siegel 은 Avaddon 의 평균 랜섬머니가 약 60 만 달러 수준이라고 밝혔다. Avaddon 의 서비스가 중단된 이유는 분명하지 않지만, 최근 주요 인프라에 대한 공격 이후 전 세계 법 집행기관과 정부가 압력을 가했기 때문인 것으로 추정된다.

최근 Colonial Pipeline 및 JBS 에 실행된 공격으로 인해 랜섬웨어는 미국 정부의 우선순위 목록에 올랐다. 대규모 랜섬웨어 작업 대부분이 러시아나 다른 CIS 국가에서 운영되는 것으로 추정되기 때문에, 바이든 대통령은 6월 16일 제네바 정상회담에서 푸틴 러시아 대통령과 최근 발생한 랜섬웨어 공격에 대해 논의할 예정인 것으로 알려졌다.

[출처]

https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

https://www.emsisoft.com/ransomware-decryption-tools/avaddon

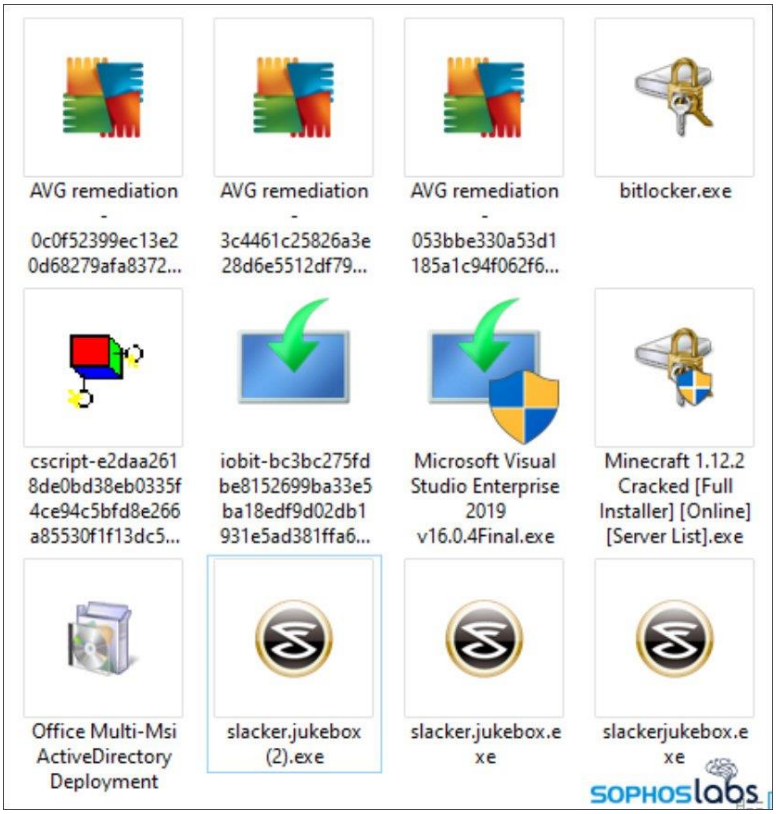
자경단 악성코드, 피해자의 불법 복제 소프트웨어 다운로드 차단해

Vigilante malware blocks victims from downloading pirated software

한 개발자가 불법 복제 소프트웨어 사이트에 접근을 차단하는 악성코드를 배포해 사용자들이 해적판 소프트웨어를 사용하지 못하도록 막고 있는 것으로 나타났다. 일반적으로 공격자들은 불법 복제 소프트웨어 및 가짜 크랙 사이트를 통해 가짜 최신 게임이나 영화를 통해 악성코드를 배포한다. 보통 이러한 방법으로 배포되는 악성코드는 인포스틸러, 랜섬웨어, 크립토마이너로 공격자가 이득을 취할 수 있는 구조다.

악성코드, The Pirate Bay 접근 차단

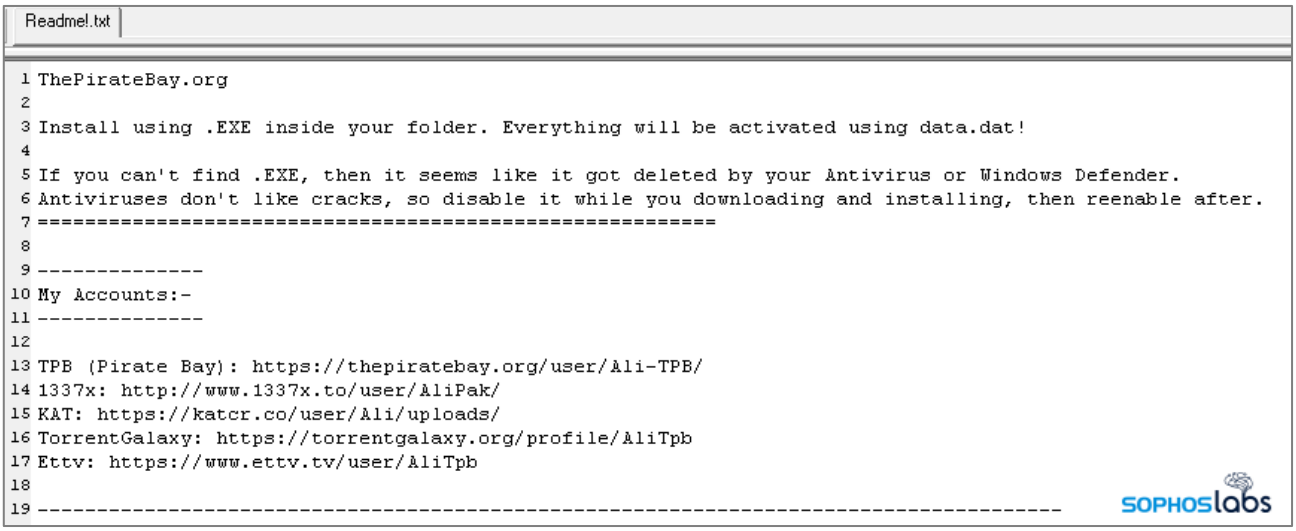
Sophos Labs 는 새로운 보고서를 통해 인기있는 해적판 소프트웨어 사이트인 The Pirate Bay 로의 접근을 차단하는 악성코드에 대한 세부 정보를 공개했다. Sophos Labs 의 수석 연구원인 Andrew Brandt 는 다음과 같이 언급했다. "이 악성코드는 비밀번호를 훔치거나 컴퓨터를 인질로 돈을 요구하는 대신, 감염된 시스템에서 호스트 파일을 수정해 수 많은 불법 복제 소프트웨어 사이트에 접근할 수 없도록 한다." Brandt 에 따르면, 이 새로운 악성코드는 디스코드 또는 불법 복제 소프트웨어 토렌트 사이트를 통해 배포되고 있다.



[이미지] 디스코드에서 호스팅된 악성코드

[이미지 출처] https://news.sophos.com/en-us/2021/06/17/vigilante-antipiracy-malware/

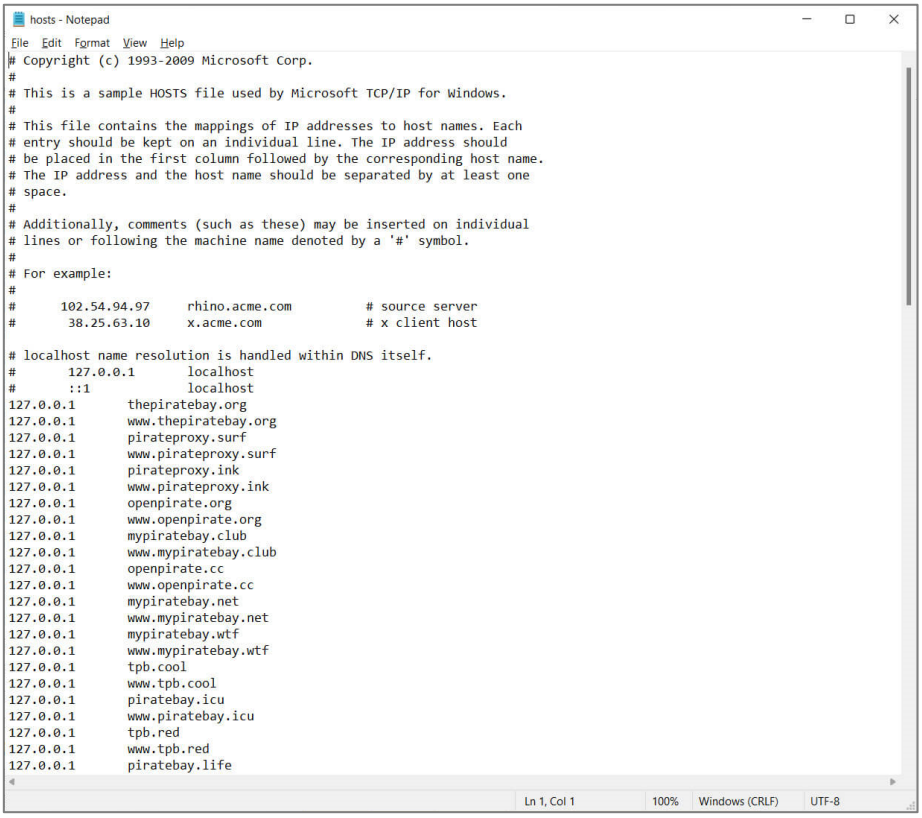
이 악성코드는 The Pirate Bay 와 같은 사이트에서도 다른 토렌트 파일과 유사한 방식으로 배포되고 있다.



[이미지] 악성 토렌트 파일 내 가짜 Readme 파일

[이미지 출처] https://news.sophos.com/en-us/2021/06/17/vigilante-antipiracy-malware/

"인스톨러에 함께 포함된 파일을 좀 더 자세히 살펴본 결과, 아카이브가 일반적으로 Bittorrent 를 공유되는 파일과 외형을 비슷하게 하고 랜덤 데이터를 추가해 해시 값을 수정하는 것 이외에는 별 다른 이점이 없다." 사용자가 악성코드 파일을 실행하면, 이는 윈도우 호스트 파일을 수정해 The Pirate Bay 와 관련된 사이트가 127.0.0.1 을 가리키도록 하는 수많은 항목을 추가한다.



[이미지] 악성코드가 수정한 호스트 파일

[이미지 출처] https://news.sophos.com/en-us/2021/06/17/vigilante-antipiracy-malware/

호스트 항목이 추가되면, 사용자가 이 중 한 사이트에 접근하려 시도할 경우 로컬 호스트로 리디렉션 되어 사이트의 실제 IP 주소에 연결할 수 없게 된다. 이로써 저작권 보호 콘텐츠의 토렌트 파일을 배포하는 사이트에 대한 접근을 효과적으로 차단할 수 있다. 또한 이 악성코드가 실행되면 공격자가 제어하는 원격 호스트에 접속해 사용자를 감염시킨 가짜 불법 복제 소프트웨어의 이름을 전송한다.

웹 서버는 보통 방문자의 IP 주소를 기록하기 때문에, 공격자는 사용자가 접근한 해적판 소프트웨어 사이트의 IP 주소와 다운로드를 시도했던 소프트웨어 또는 영화 이름을 받아올 수 있게 된다. 이러한 정보를 어떻게 사용할지는 알 수 없지만, 공격자는 이를 ISP, 저작권 기관, 경찰 등에 신고할 수 있다. 또한 이메일을 통한 협박 공격에 이 정보를 사용할 가능성도 있다. 공격자는 자신의 요구를 들어주지 않을 경우 사용자의 불법 행위를 공개하겠다고 협박할 수 있다. Brandt 는 이 악성코드 캠페인이 2020 년 10 월부터 2021 년 1 월 사이에 활동했다고 밝혔다. 이 악성 토렌트 파일은 사용자가 해당 파일이 악성/가짜인 것을 발견한 후 시딩을 중단해 배포가 중단된 것으로 나타났다.

[출처]

https://www.bleepingcomputer.com/news/security/vigilante-malware-blocks-victims-from-downloading-pirated-software/

https://news.sophos.com/en-us/2021/06/17/vigilante-antipiracy-malware/

(주)이스트시큐리티

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