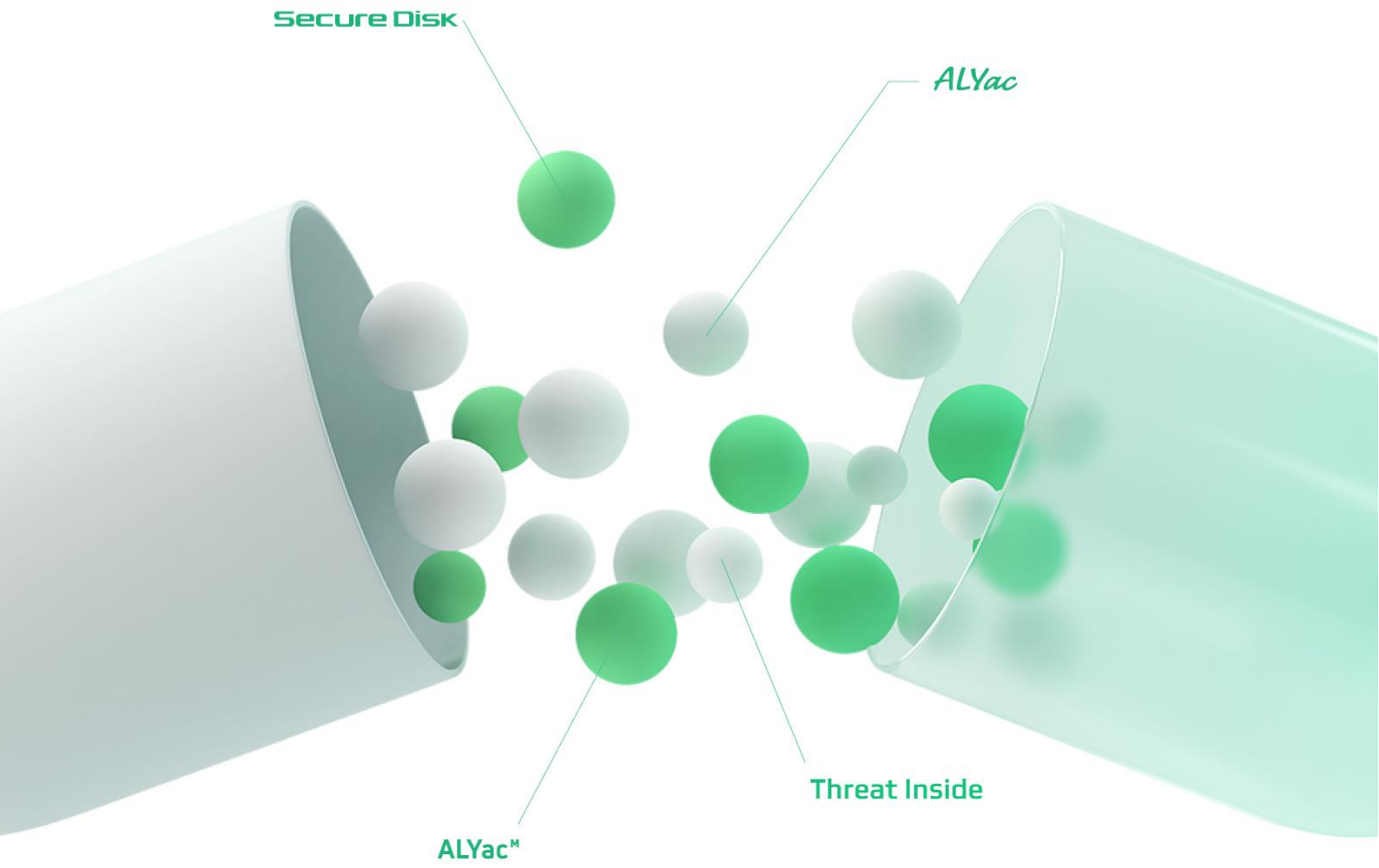
이스트시큐리티
보안동향보고서

No.152
2022/05/30

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외보안동향을 확인하세요.



이스트시큐리티 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

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

1. 악성코드 동향

2022년 4월에는 새로운 악성코드들이 많이 발견되었습니다.

RAT, 스파이웨어, 랜섬웨어 등의 다양한 기능을 갖고 있는 새로운 Borat 악성코드가 다크웹에서 발견되었습니다. 뿐만 아니라 AWS Lambda 클라우드 환경을 노리기 위해 특별히 개발된 최초의 악성코드와 현재 개발단계로 추정되는 고도화된 악성코드로, 여러 사이버 공격자들이 사용하고 있는 Bumblebee 악성코드도 발견되었습니다.

2021년 11월 활동을 재개한 이후 지속적인 성장중인 Emotet 악성코드의 공격방식이 다변화 하고 있습니다. 최근에는 더 이상 Microsoft Office 매크로를 사용하지 않고, PowerShell 명령이 포함된 윈도우 바로 가기 파일(.LNK)을 사용하기 시작하였습니다. Emotet은 페이로드를 다운로드하는 명령을 빌드하기 위해 VBS(Visual Basic Script) 코드와 함께 .LNK 파일을 사용했기 때문에, 이는 새로운 전략은 아니지만 윈도우의 바로가기를 통해 직접 PowerShell 명령어를 실행한 경우는 이번이 처음입니다. 이는 자동화된 탐지를 우회하려는 시도로 추측되고 있습니다.

윈도우 도움말 파일(chm)을 이용한 악성 메일도 지속되었습니다.
3월 말부터 시작된 악성 chm 파일을 이용한 공격은 4월에도 지속되었으며, '질병예방 및 자가진단', '20대 대선 결과와 향후 전망' 등 사용자들이 관심을 가질만한 다양한 주제의 압축파일을 첨부하여 사용자들의 클릭을 유도하였습니다. 해당 압축파일 내에는 정상 워드파일과 함께 rar로 압축되어 있는 악성 윈도우 도움말(chm) 파일이 포함되어 있으며, 사용자가 chm 파일을 실행하면 powershell을 이용하여 c2에 접속하여 추가 파일을 내려받습니다.

이 밖에도, 우크라이나의 에너지 시설과 국가기관 등이 지속적으로 사이버 공격을 받고 있어, 러시아와 우크라이나 전쟁이 오프라인뿐만 아니라 사이버 영역에서도 지속되고 있음을 알 수 있습니다.

악성코드 및 해킹 공격들이 점점 정교화 되고 고도화 되면서 그 위협성 역시 점점 증가하고 있습니다. 또한 신규 혹은 이미 발견된 취약점을 악용한 공격들도 꾸준히 발생하고 있는 만큼, 보안담당자는 신규 취약점 등을 꾸준히 모니터링 하고, 주기적인 취약점 점검 및 보안패치를 통하여 잠재적인 위험의 가능성을 낮추려는 노력이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2022년 4월의 감염 악성코드 Top 15 리스트에서는 국내 광고 소프트웨어를 설치하는 Hosts.media.opencandy.com 악성코드가 665,984건에서 541,661건으로 약 18.6% 증가하였고, 지속적으로 1위를 유지하고 있습니다.

또한 파일 감염형 악성코드 Worm.IM-VB.as, Win32.Neshta.A, Trojan.HTML.Ramnit.A 등이 새롭게 Top리스트에 등장하였고, 특히 Trojan.HTML.Ramnit.A는 HTML파일을 변조하여 또다른 Trojan 악성코드를 사용자PC에 드롭시켜 사용자PC에 저장된 중요 정보나 브라우저 쿠키 값 등을 탈취 / 봇넷을 생성할 수 있는 악성코드이다.

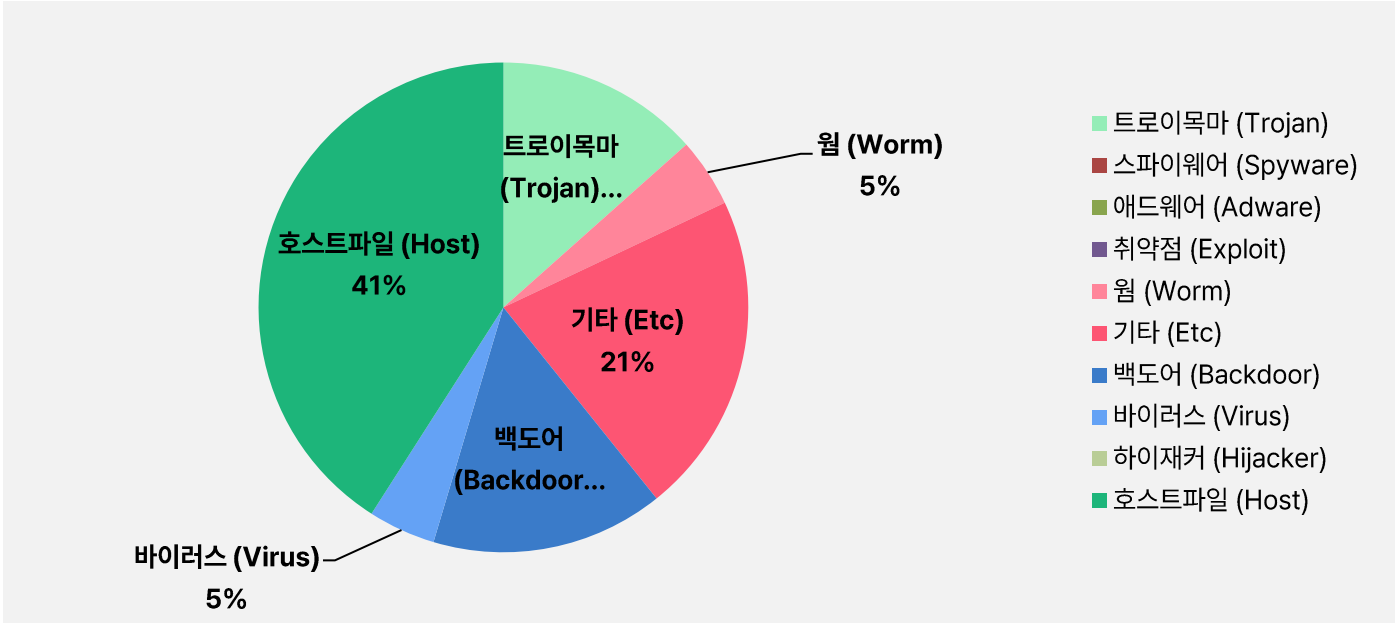
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	541,661
2	-	Backdoor.Generic.792814	Backdoor	203,256
3	-	Misc.HackTool.AutoKMS	ETC	77,753
4	New	Worm.IM-VB.as	Worm	60,132
5	New	Win32.Neshta.A	Virus	58,829
6	↓1	Trojan.Damaged.PE	Trojan	58,260
7	↓1	Misc.HackTool.KMSActivator	ETC	42,920
8	↓4	Trojan.Lisp.Agent.F	Trojan	42,900
9	↑4	JS:Trojan.Cryxos.5175	Trojan	42,359
10	↓3	Application.Hacktool.KMSActivator.AI	ETC	37,190
11	↓2	Application.Hacktool.KMSActivator.HJ	ETC	34,663
12	New	Trojan.HTML.Ramnit.A	Trojan	34,087
13	↓5	Application.Hacktool.KMSActivator.HA	ETC	31,925
14	New	Gen:Variant.Razy.864420	ETC	28,764
15	↓1	Application.Hacktool.KMSAuto.AT	ETC	28,244

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022년 4월 01일 ~ 2022년 4월 30일

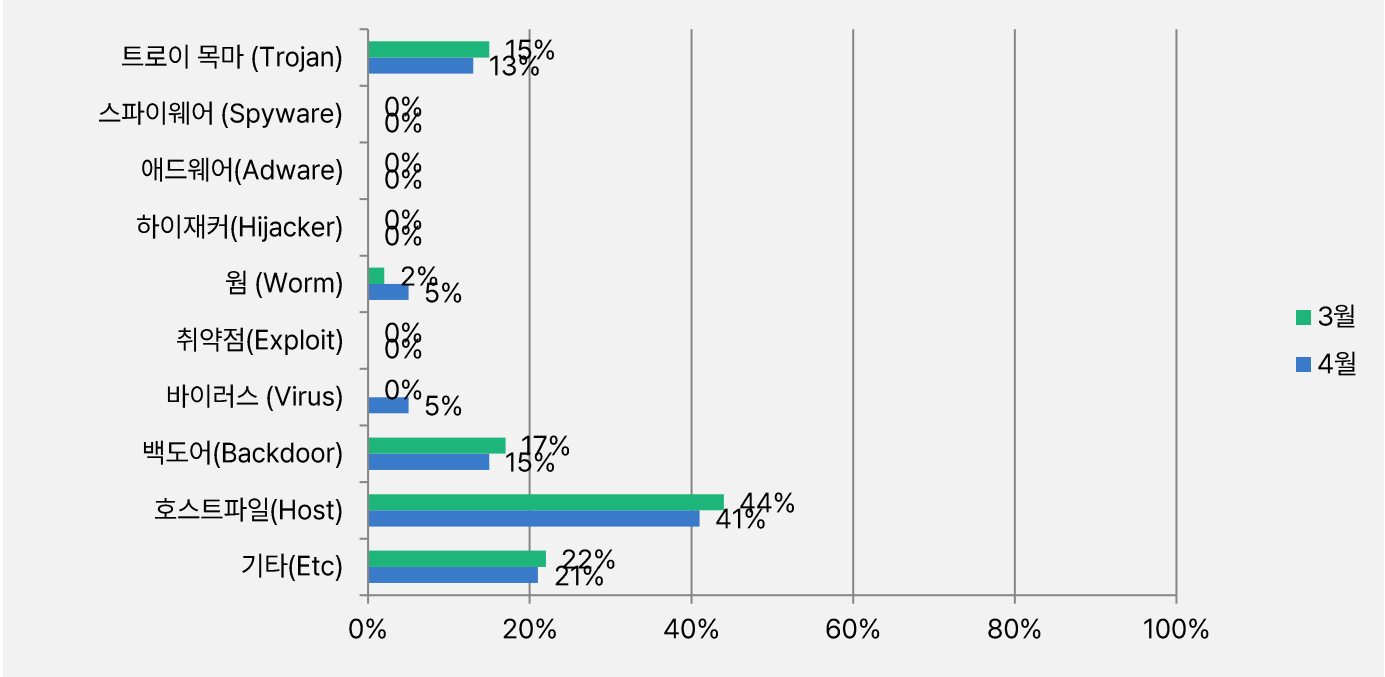
악성코드 유형별 비율

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



카테고리별 악성코드 비율 전월 비교

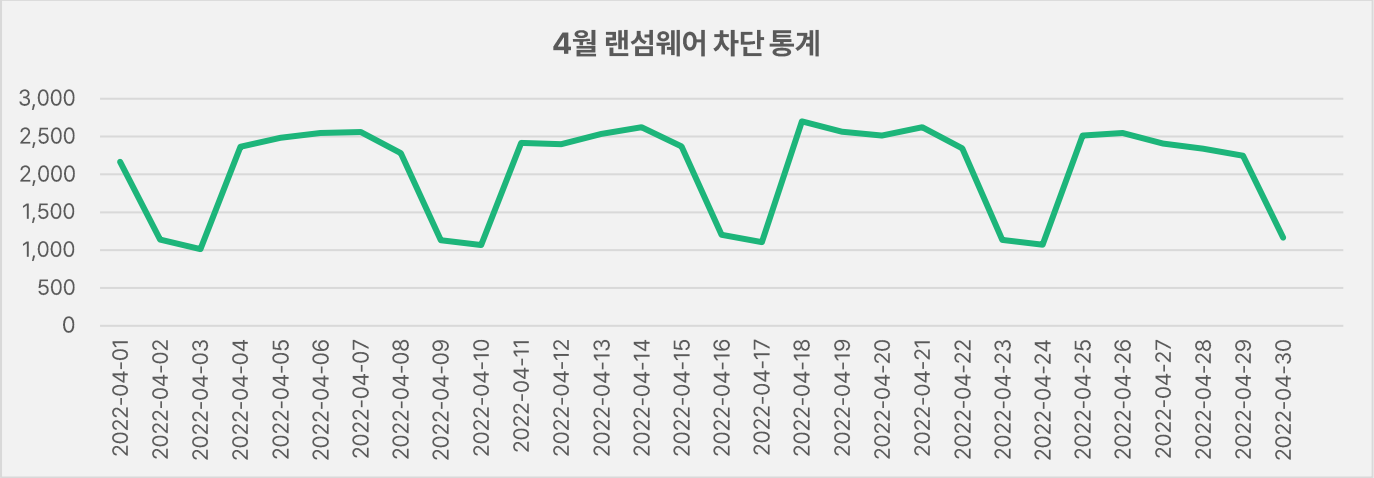
2022년 4월에는 지난 3월과 비교하여 기타(ETC)와 호스트파일(Host) 유형이 각각 1%, 3% 감소했으며, 백도어(Backdoor), 트로이목마(Trojan) 유형은 전월 대비 비슷한 15%,13%를 기록하였고 웜(Worm) 유형이 5%로 지난 달에 비해 3% 증가하였다. 바이러스(Virus) 유형이 새롭게 5% 비율의 탐지율을 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

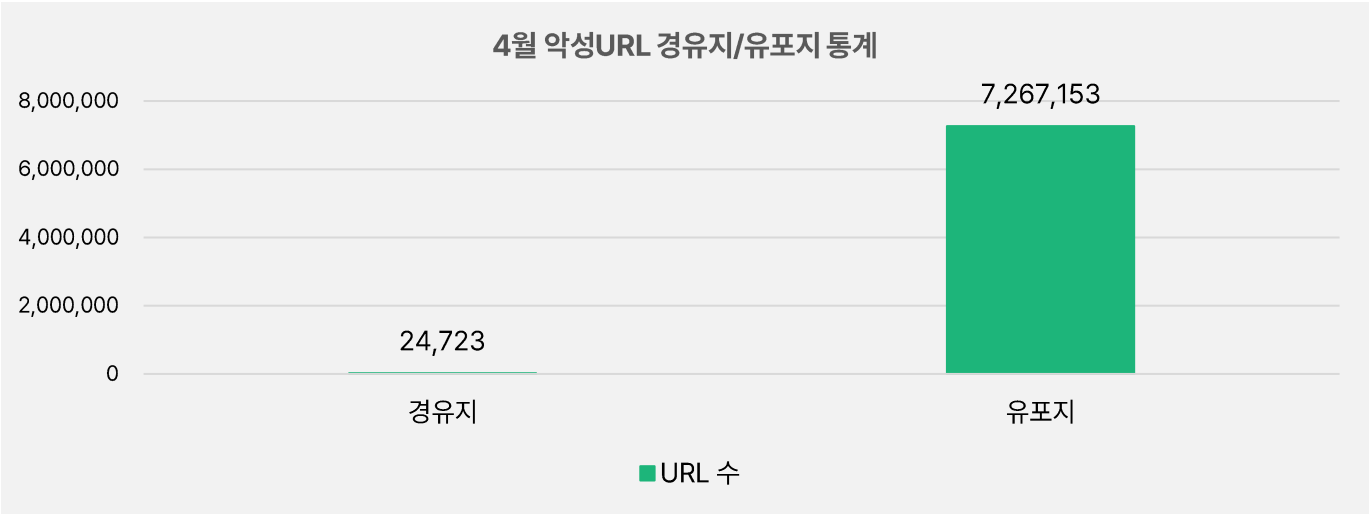
4월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 4월 1일부터 4월 30일까지 총 61,582건의 랜섬웨어 공격 시도가 차단되었다. 3월의 랜섬웨어 공격 건수인 63,047건에 비해 약 2.3% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 4월 한 달간 총 7,291,876건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 3월 한 달간 확인되었던 7,490,660의 악성코드 경유지/유포지 URL 수에 비해 약 2.6% 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. CBPR(Cross Border Privacy Rule) 인증제도란?

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

1. CBPR(Cross Border Privacy Rule) 인증제도란?

22년 5월 3일부터, 개인정보보호위원회는 한국인터넷진흥원(KISA)와 공동으로 CBPR 인증 제도를 도입,운영한다고 밝혔습니다. 이로서, 국내 기업들이 해외 기관을 통하지 않고 CBPR인증을 받을 수 있게 되었습니다.

이에 이스트시큐리티에서는 CBPR인증은 무엇이며 어떠한 효용성이 있는지 간략히 설명해 드리고자 합니다.

CBPR(Cross Border Privacy Rule)이란?

CBPR이란, 국경간 프라이버시보호규칙(Cross Border Privacy Rule)의 약자로 2011년 APEC이 전자상거래의 활성화와 회원국 간 안전한 개인정보의 상호 이전을 위해 개발한 글로벌 개인정보보호 자율인증제도 입니다.

APEC 회원국에 한하여 CBPR 가입 신청이 가능하며, 현재(22년 5월 현재)) 회원국은 총 9개 국가(미국, 멕시코, 일본, 캐나다, 한국, 호주, 싱가포르, 대만, 필리핀) 입니다.

CBPR 인증 기준 요구사항

'APEC 프라이버시 프레임워크(APF)'에 포함된 9개 원칙을 기반으로 개발되었으며, 총 50개 인증 기준으로 구성되어 있습니다.

APEC Privacy Framework	설명	CBPR 인증 기준 (50개)
고지 (Notice)	'사전 혹은 동시'에 고지를 제공할 것을 규정하고 있고, 경우에 따라 '사후 고지' 가능	개인정보보호 정책 고지 항목, 고지 방법 등
수집제한 (Collection Limitation)	수집 목적에 관련된 정보를 합법적이고 공정하게 수집하고, 적절한 경우 동의를 받아야 함	개인정보 수집 방법, 수집 최소화, 합법적 수집 등
개인정보 이용 (Uses of Personal Information)	수집 목적과 양립 가능하거나 관련된 목적으로 이용	수집 목적 내 이용,위탁,제3자 제공 등
선택 (Choice)	적절한 경우 정보주체에게 수집, 이용, 제공에 대한 선택권 부여	정보주체의 수집, 이용, 제공에 대한 선택권 제공방법 등
개인정보의 무결성 (Integrity of Personal Information)	정보의 정확성, 완정성, 최신성 확보	개인정보의 최신, 정확, 완전성을 위한 정정, 수탁자 통지 등
보안조치 (Security afeguards)	위험 발생 가능성과 심각성, 정보의 민감성에 비례하여 적절히 조치 * 구체적 보호조치 기준 없음	개인정보의 민감성, 침해가능성 및 침해의 심각성에 비례한 보호조치, 보호조치에 대한 평가 등
열람,정정 (Access and Correction)	정보주체의 요청이 있을 시 개인정보의 열람,정정 등이 가능하나, 과도한 비용이 수반되거나 상업적 비밀로 보호되어야 하는 경우 제외	정보주체의 열람, 정정, 삭제 요청에 대한 절차 등
책임성 (Accountability)	개인정보를 이전하는 경우, 동의를 받거나 개인정보를 이전받는 기관(개인)의 보호 수준을 실사하고 합리적 조치 이행	책임자 지정, 민원처리 및 피해구제 절차, 수탁자 및 제3자에 대한 관리,감독 방법 등
피해 구제 (Preventing Harm)	구제조치는 피해의 개연성과 심각성에 비례하여 취해져야 함	(책임성 등 다른 항목에 '피해 구제'에 대한 사항 내포)

CBPR과 GDPR

GDPR은 유럽연합(EU)의 개인정보보호 법령으로, 회원국 간 개인정보보호 법제가 달라 기업들의 활동에 문제가 발생하자 강력하고 통일적인 개인정보보호 규제를 하기 위하여 제정하였습니다.

GDPR은 유럽 내 기업에만 적용되는것이 아니라, EU역내에 자회사를 두었거나 EU에 서비스를 제공하고 개인정보처리에 대한 위탁을 받은 모든 기업들에게 적용됩니다.

▶ GDPR 전격 시행! 데이터 보안 관점에서 필요한 대비책은?

CBPR과 GDPR의 주요 개념을 비교해 보자면 다음과 같습니다.

구분	CBPR	GDPR
목적	회원국 간 정보 흐름을 원활하게 하고 지속적인 무역 및 경제 성장을 보장하기 위한 효과적인 개인정보 보호를 목표로 함	자연인들의 기본적 권리와 자유, 특히 개인정보보호건의 보호와 개인정보의 자유로운 이동의 보장을 목적으로 함
적용범위	APEC 회원국 법률 범위 내	EU 회원국 법률 범위 내
	개인정보의 수집, 보유, 처리, 사용, 전송 또는 공개하는 공공 및 개인 또는 민간 조직에 적용	- 자동화된 방법으로 전체/부분적으로 개인정보를 처리하는 경우 적용 - EU 역내 처리 여부에 관계없이 EU 내의 정보처리자 또는 수탁처리자의 사업장의 활동에 따른 개인정보 처리에 적용 - 특히 EU내에 설립되지 않은 정보처리자 또는 수탁처리자의 경우라도, EU 역내에 거주하는 정보주체에게 재화나 서비스를 제공하는 경우나 정보주체의 행동을 모니터링 하는 경우 적용
개인정보	식별되거나 식별 가능한 개인에 관한 모든 정보	식별된/식별 가능한 자연인과 관련된 일체의 정보
개인정보처리자	개인정보의 수집, 보유, 처리, 사용, 전송 또는 공개하는 개인이나 조직	개인정보의 처리목적 및 수단을 결정하는 자연인 또는 법인, 공공기관, 기타 단체
수탁처리자	적용되지 않음	적용됨
	CBPR은 개인정보처리자에게 적용되고 수탁처리자에게는 적용되지 않음	- 제28조(수탁처리자) - 제29조(정보처리자 및 수탁처리자의 권한에 따른 처리)

CBPR 효용성

CBPR 인증은 글로벌 인증으로, 인증획득을 통해 APEC 기준의 개인정보보호 체계를 갖췄다는 인정을 받을 수 있습니다.

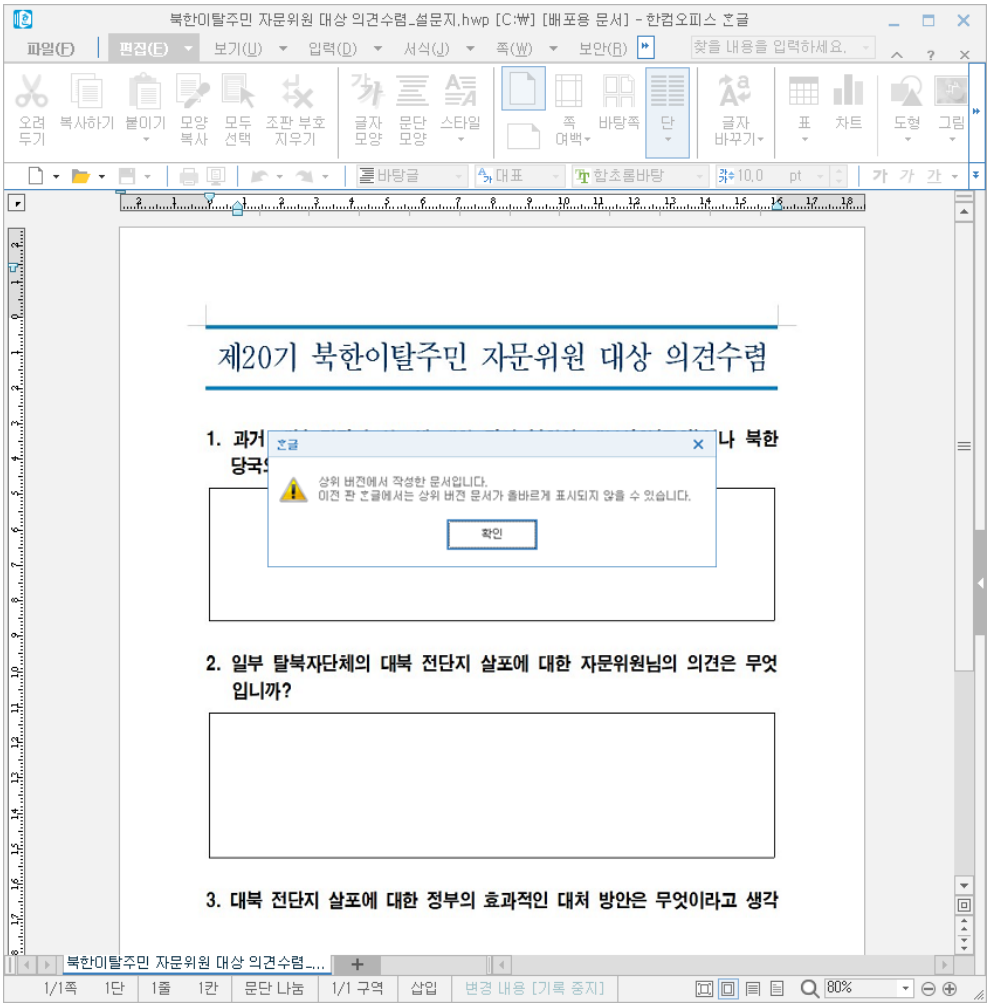
또한 일본, 싱가포르의 경우 CBPR을 자국의 개인정보보호법과 동등한 수준의 보호체계로 인정하였으며, 이에 CBPR인증 기업은 이러한 국가들에서 정보주체 동의 등 추가적인 절차 없이 개인정보의 국경간 이전이 가능하여 업무 효율성 증대가 기대됩니다.

CBPR의 인증 기준 중 대부분이 국내의 개인정보보호법에 포함되어 있는 내용이기 때문에, ISMS-P 의무 인증 기업이라면 인증심사를 통과 하는데 큰 어려움이 없을 것으로 예상됩니다.

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

북한이탈주민(탈북민) 자문위원들에게 의견을 수렴하는 내용처럼 위장한 HWP 악성 문서 기반 北 연계 해킹 공격이 발견되어 사용자들의 각별한 주의가 필요합니다.

이번 공격은 마치 북한이탈주민 자문위원을 대상으로 한 의견수렴 설문지처럼 위장한 것이 특징이며, 공격자는 HWP 한글 문서 내부에 OLE(개체 연결 삽입) 기능을 악용했습니다.

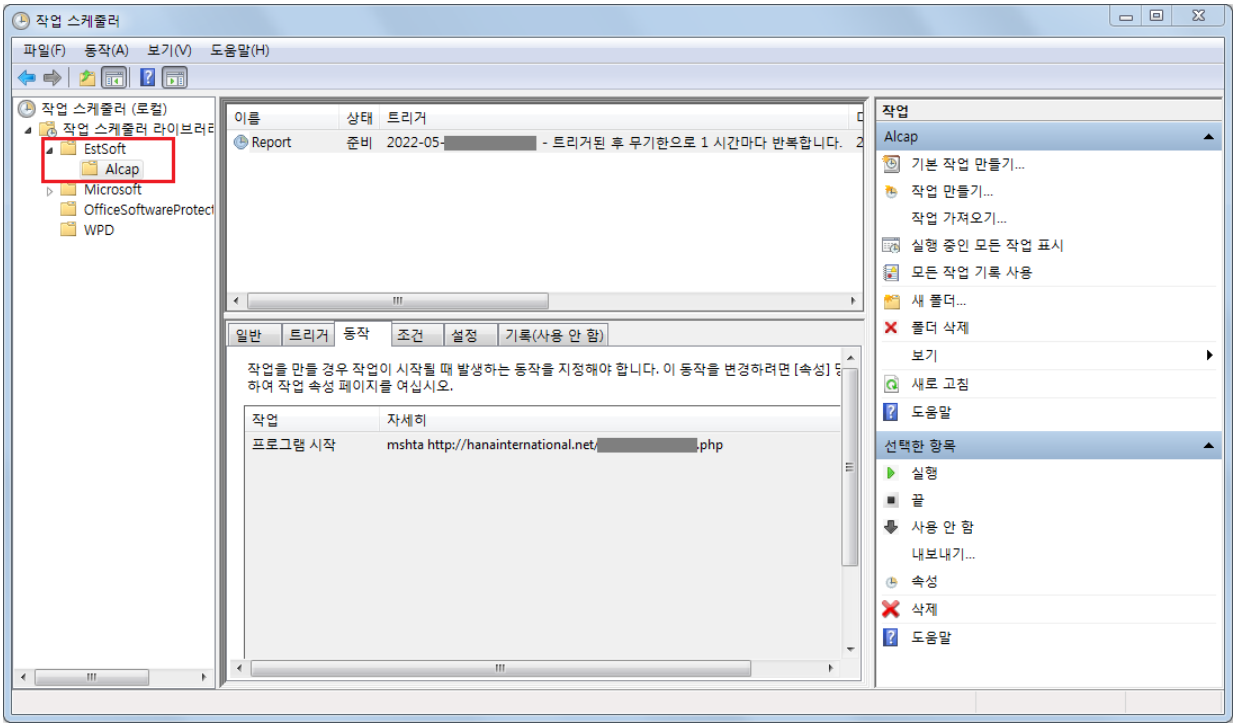


[그림 1] 북한이탈주민 자문위원 대상 의염 수렴 문서로 위장한 악성파일 화면

공격자는 수신자가 문서를 실행하면 '상위 버전에서 작성한 문서입니다.' 등의 가짜 메세지 창을 띄워 사용자의 클릭을 유도하며 사용자가 확인 버튼을 누르면, HWP 파일 내 삽입되어 있는 OLE 기능을 통하여 배치(Bat) 파일과 파워셸(Powershell) 명령어를 통해 국내 특정 서버로 통신을 시도합니다.

해당 메세지 창은 정상 HWP 문서에서도 자주 볼 수 있는 문구이기 때문에 사용자들이 별 의심없이 [확인]버튼을 클릭할 수 있습니다. 이는 HWP의 보안 취약점이 아니기 때문에 버전과 상관 없이 한컴 오피스를 사용하는 사용자들이 공격 대상이 될 수 있어 이러한 별도이 메세지 창이 뜨면 클릭 전 각별한 주의를 기울여야 합니다.

주목할 점은, 명령제어(C2) 서버로 통신을 시도할 때, 외부에 노출되는 것을 숨기기 위하여 작업 스케줄러에 잠복 기능처럼 동작 조건을 추가했으며, 마치 이스트소프트 프로그램처럼 위장하는 수법을 사용했다는 것입니다.



[그림 2] 이스트소프트 사칭으로 작업스케줄러에 추가된 악성 명령 화면

한편, 자유북한운동연합이 지난 4월 25일과 26일 이틀에 걸쳐 경기도 김포지역에서 20개의 대형 애드벌룬으로 약 100만 장의 대북 전단을 살포했다고 주장하고 나선 바 있는데, 이번 악성 파일은 마치 해당 내용의 의견을 수렴하는 것처럼 사칭함으로써 공격에 시기적절하게 활용되었습니다.

공격자들은 이처럼 실제 언론 등을 통해 알려진 내용을 그대로 차용해 공격 효과를 보다 극대화시키는 전략을 사용하고 있는 점에 주목해야 합니다.

이번 공격은 지난 2월 유엔인권사무소 사칭 피싱 공격과 마찬가지로 국내 서버를 해킹 중간 거점으로 활용했으며, 동일한 작업 스케줄러 이름과 'PEACE', 'Lailey' 아이디 등을 사용된 것을 확인하였습니다.
이번 공격에 사용된 HWP 공격 수법과 전술 명령 등은 이전의 북한 연계 사이버 공격 사례와 일치한 것으로 분석돼, 배후에 북한 사이버 위협 조직이 있는 것으로 지목되었습니다.

한편, 이스트시큐리티 ESRC는 이와 관련된 사이버 위협 정보를 한국인터넷진흥원(KISA) 등 관계 당국과 긴밀히 공유해 기존에 알려진 위협이 확산되지 않도록 협력을 유지하고 있습니다.

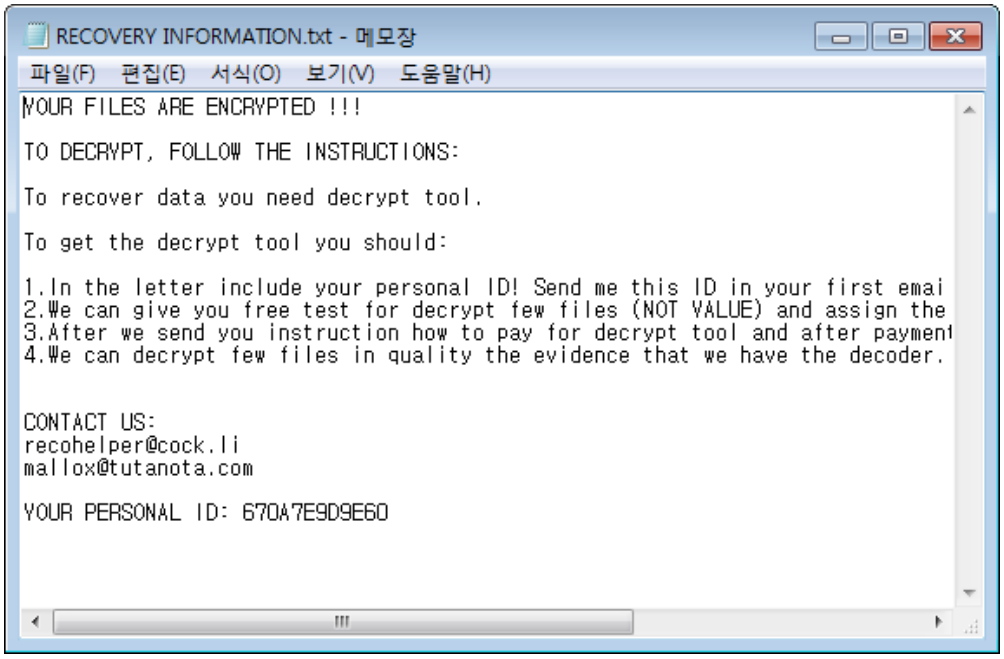
3

악성코드 분석 보고

[Trojan.Ransom.Filecoder] 악성코드 분석 보고서

작년 하반기부터 활동중인 Mallox 랜섬웨어는 2022년 3월 랜섬웨어 패밀리들을 대상으로 진행된 통계에서 기업 타겟 랜섬웨어로 1위를 차지하였다.

현재까지 국내에 감염된 사례는 보고된 적 없지만 봇넷, 네트워크 유포, 취약한 암호 등 다양한 방식을 통해 유포 중인 것으로 알려진 Mallox 랜섬웨어를 분석하고자 한다.



[그림] 랜섬노트 화면

Mallox 랜섬웨어는 사용자 PC의 데이터를 암호화하여 금전을 요구하는 악성코드이다. 시스템 언어가 러시아어, 카자흐어, 벨라루스어, 우크라이나어, 타타르어일 경우 암호화 작업 없이 프로세스를 종료하는 것과 사용자의 APR table에서 IP 주소와 관리 목적의 공유 폴더를 사용하여 랜섬웨어를 전파한다는 특징이 있다.

또한 로컬 드라이브와 네트워크 드라이브로 연결된 모든 파일을 암호화 대상에 포함하고 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

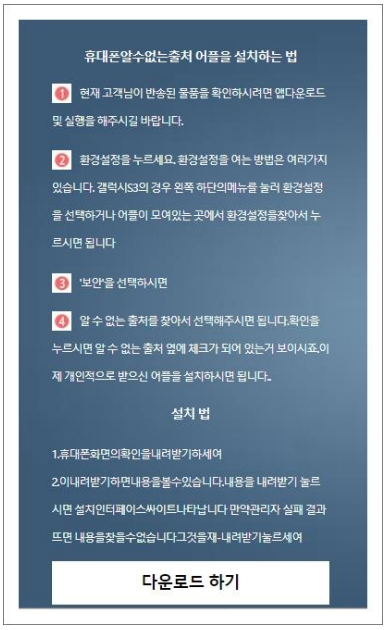
따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

현재 알약에서는 **'Trojan.Ransom.Filecoder'**으로 진단하고 있다.

[Trojan.Android.SmsSpy] 악성코드 분석 보고서

스미싱 공격은 다양한 키워드를 활용하여 수행한다. 그러나 초창기 스미싱 공격부터 현재까지 꾸준하게 공격자들이 선호하는 키워드가 있다. "택배" 키워드이다.

초창기 스미싱 공격의 주요 키워드는 "청첩장", "돌잔치", "택배" 등이었다. 그러나 "택배" 이외의 키워드들은 시기나 사회의 관심사와 연관된 키워드로 지속적으로 변경이 되었으나 "택배" 키워드만큼은 꾸준하게 활용되고 있다.



[그림] 악성 앱 다운로드 페이지

택배 스미싱은 스미싱 공격의 초기부터 발견되기 시작하여 현재까지 꾸준하게 발견되고 있다. 이는 택배 스미싱이 공격자들에게 매우 효과적인 공격 방법이라는 것을 알 수 있다. 이렇게 악성 앱이 개인 정보를 탈취하게 되면 탈취한 개인 정보를 활용하여 2차 공격을 가하게 되고 결국은 금전 탈취를 시도하게 된다.

이런 스미싱 공격은 사용자가 충분한 주의를 기울이지 않는다면 부지불식간에 당하기 마련이기에 사용자의 예방 노력이 무엇보다 중요하다. 앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약M과 같은 신뢰할 수 있는 백신을 사용해야 한다.

따라서, 공식 스토어를 이용하더라도 신뢰할 수 있는 앱 제작자인지 확인이 필요하며 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫걸음이다.

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

4

글로벌 보안 동향

새로운 원격 접속 트로이목마인 Borat 발견

New Borat remote access malware is no laughing matter

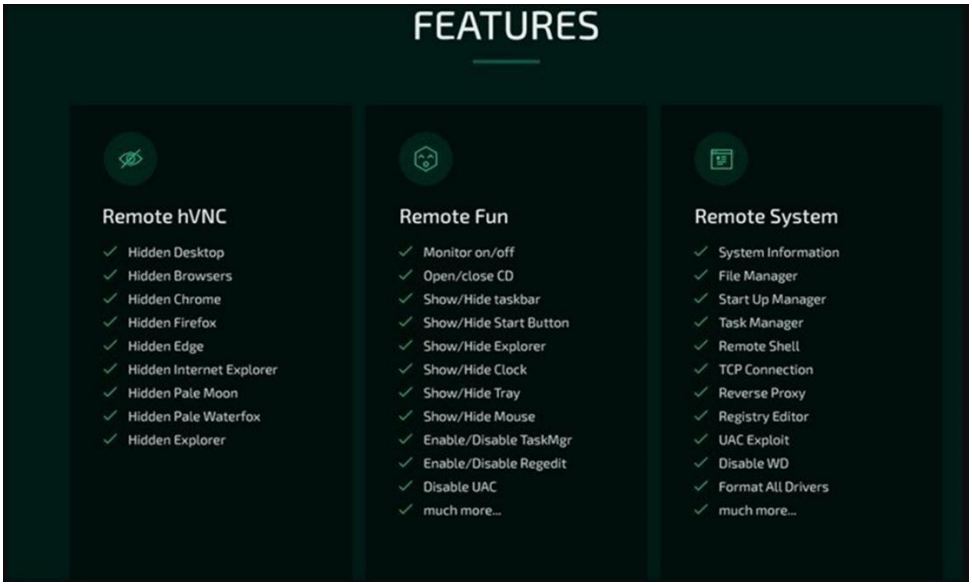
새로운 원격 접속 트로이목마(RAT)인 Borat이 다크넷 마켓에서 발견되었습니다. 이는 DDoS 공격, UAC 우회, 랜섬웨어 배포를 수행하기 위한 사용이 쉬운 기능을 제공합니다.

[이미지 출처] https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/

원격 공격자가 Borat을 사용할 경우 피해자의 마우스와 키보드를 완전히 제어하고 파일, 네트워크 지점에 접근하고 그들의 모든 존재 흔적을 숨길 수 있습니다.

이 악성코드는 운영자가 컴파일 옵션을 선택하는 방식을 통해 고도로 커스텀된 공격에 정확히 필요한 기능을 제공하는 작은 페이로드를 생성하도록 돕습니다.

Cyble의 연구원들은 실제 공격에서 Borat을 발견한 후 악성코드의 샘플을 채취해 이를 연구할 수 있었습니다.

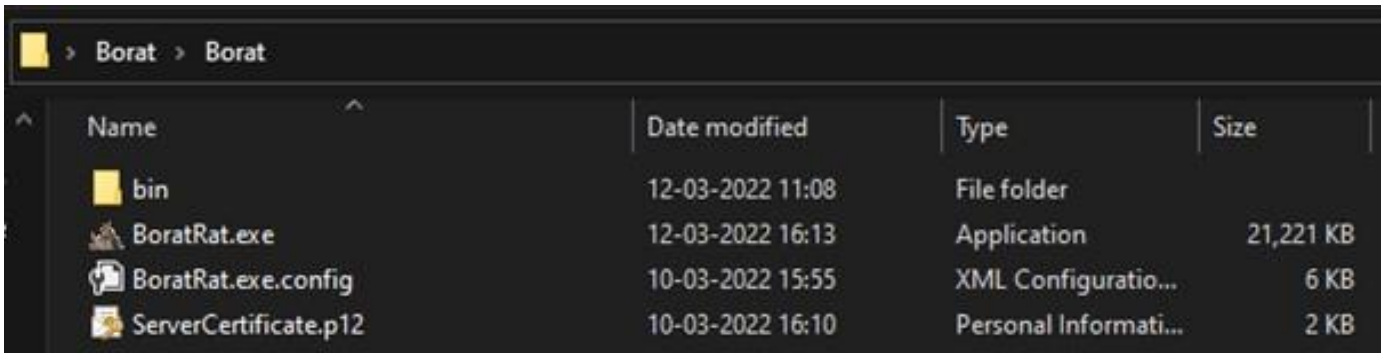


[그림] Borat의 기능 중 일부

[이미지 출처] https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/

폭 넓은 기능

Borat RAT이 판매되고 있는지, 공격자들 사이에서 자유롭게 공유되는지는 확실하지 않습니다. Cycle은 이 악성코드가 빌더, 멀웨어 모듈, 서버 인증서가 포함된 패키지 형태로 제공된다고 밝혔습니다.



[그림] Borat RAT 압축파일 내 파일

[이미지 출처] https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat

이 트로이 목마의 기능은 아래와 같습니다.

키로깅 – 키 입력 모니터링 및 기록 후 txt 파일에 저장

랜섬웨어 – 피해자의 시스템에 랜섬웨어 페이로드를 배포하고 Borat을 통해 랜섬노트 자동 생성

DDoS – 해킹된 시스템의 리소스를 통해 가비지 트래픽을 타깃 서버로 전송

오디오 녹음 – 가능한 경우 마이크를 통해 오디오를 녹음하고 wav 파일에 저장

웹캠 녹화 – 가능한 경우 웹캠을 통해 비디오 녹화

원격 데스크톱 – 숨겨진 원격 데스크톱을 시작해 파일 작업 수행, 입력 장치 사용, 코드 실행, 앱 실행 등 수행

역방향 프록시 – 원격 운영자의 신원이 노출되는 것을 방지하기 위한 역방향 프록시 설정

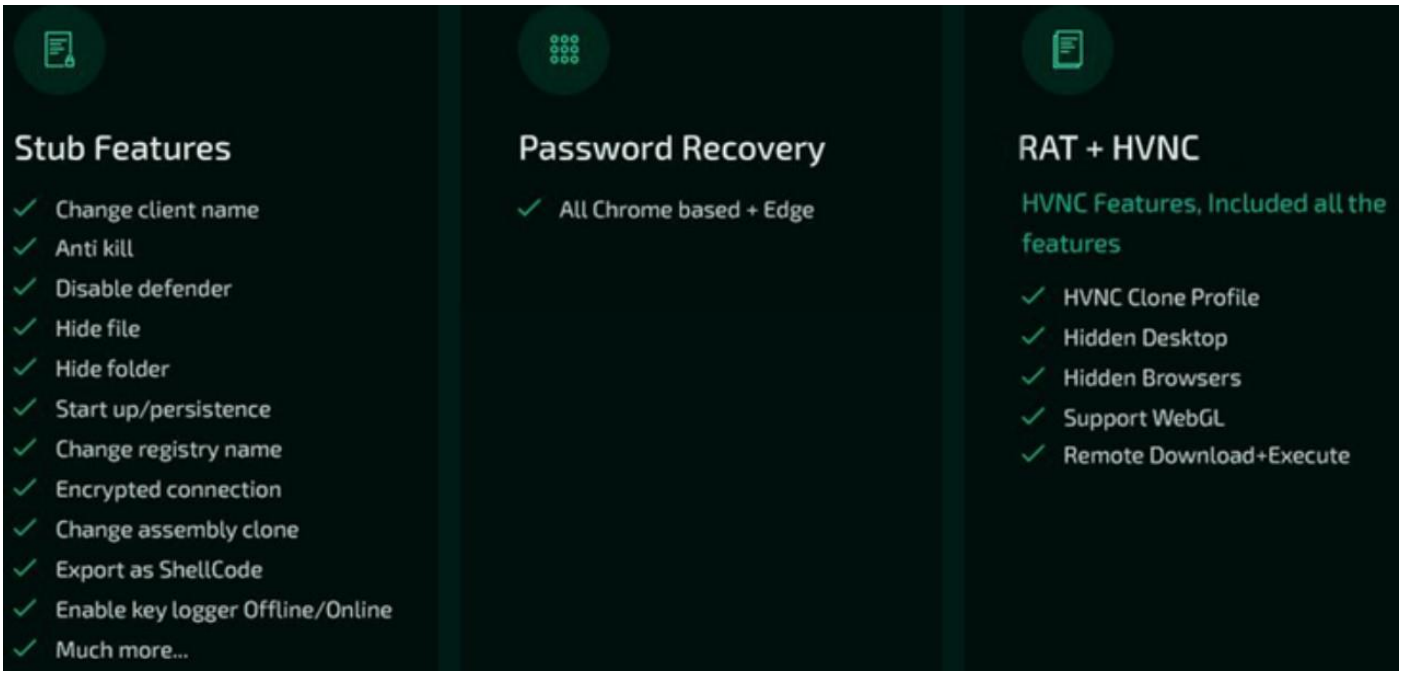
장치 정보 – 기본 시스템 정보 수집

프로세스 할로잉(Process hollowing) – 정식 프로세스에 악성코드를 삽입하여 탐지 회피

크리덴셜 탈취 - Chromium 기반 웹 브라우저에 저장된 계정 크리덴셜 탈취

Discord 토큰 탈취 – 피해자의 Discord 토큰 탈취

기타 기능 – 오디오 재생, 마우스 버튼 변경, 바탕 화면 숨기기, 작업 표시줄 숨기기, 마우스 홀딩, 모니터 끄기, 빈 화면 표시, 시스템 행 등으로 피해자를 방해하고 혼란스럽게 하기



[그림] Borat의 추가 기능
[이미지 출처] https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/

Borat은 위의 기능으로 인해 본질적으로 RAT, 스파이웨어, 랜섬웨어가 되기 때문에 기기에서 다양한 악성 활동을 수행할 수 있습니다.

Bleeping Computer에서 확인 결과 해당 페이로드 실행 파일이 최근 AsyncRAT로 식별되었음을 발견했습니다. 따라서 제작자는 이를 기반으로 작업했을 가능성이 큽니다.

공격자는 일반적으로 게임 및 애플리케이션의 크랙으로 위장한 파일을 통해 악성 툴을 배포하기 때문에, 토렌트 또는 불법 사이트 등 신뢰할 수 없는 출처에서 다운로드 하지 않는 것이 좋습니다.

[출처]
https://www.bleepingcomputer.com/news/security/new-borat-remote-access-malware-is-no-laughing-matter/
https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/ (IOC)

페이스북, 인스타그램, 트위터 계정을 훔치는 새로운 FFDroider 악성코드 발견

New FFDroider malware steals Facebook, Instagram, Twitter accounts

브라우저에 저장된 크리덴셜과 쿠키를 훔치고 피해자의 소셜 미디어 계정을 탈취하는 새로운 인포스틸러인 FFDroider가 발견되었습니다.

소셜 미디어 계정, 특히 인증된 계정은 공격자가 가상 화폐 사기 및 악성코드 배포를 포함한 다양한 공격에 사용할 수 있기 때문에 해커들에게 인기가 많습니다.

이러한 계정은 소셜 사이트의 광고 플랫폼에 접근할 수 있을 경우 공격자가 훔친 크리덴셜을 통해 악성 광고를 게시할 수 있기 때문에 훨씬 더 매력적입니다.

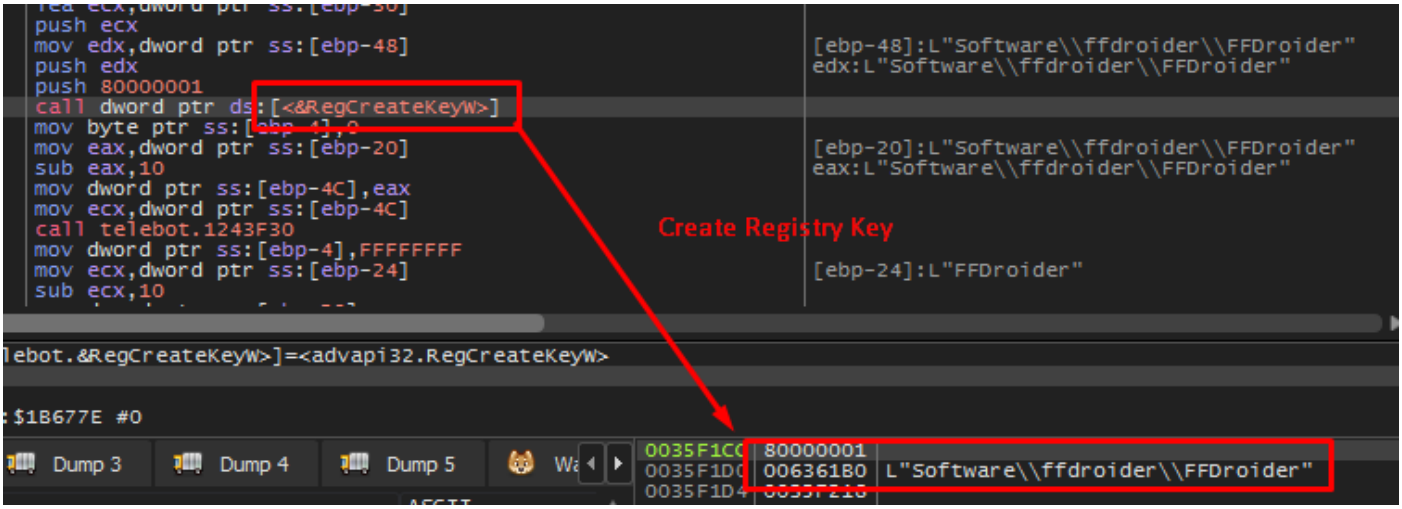
소프트웨어 크랙 통해 배포돼

Zscaler의 연구원들은 새로운 인포 스틸러를 추적하던 중 최근 샘플을 기반으로 한 자세한 기술 분석을 발표했습니다.

많은 악성코드와 마찬가지로 FFDroider는 소프트웨어 크랙, 무료 소프트웨어, 게임, 기타 파일을 토렌트 사이트에서 다운로드하여 확산됩니다.

해당 파일을 실행하면 FFDroider도 설치되지만, 이는 탐지를 피하기 위해 Telegram 데스크톱 앱으로 위장합니다.

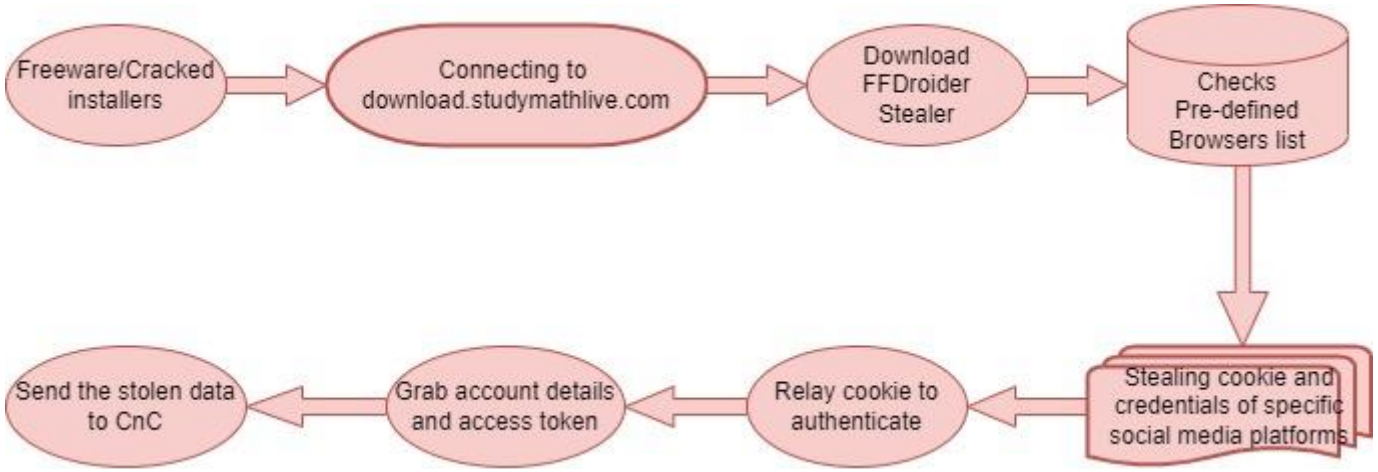
일단 실행되면, 악성코드는 "FFDroider"라는 윈도우 레지스트리 키를 생성합니다.



[그림] 감염된 시스템에 레지스트리 키를 추가하는 FFDroider

[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

Zscaler의 연구원은 악성코드가 피해자의 기기에 설치되는 방식을 보여주는 플로우 차트를 공개했습니다.



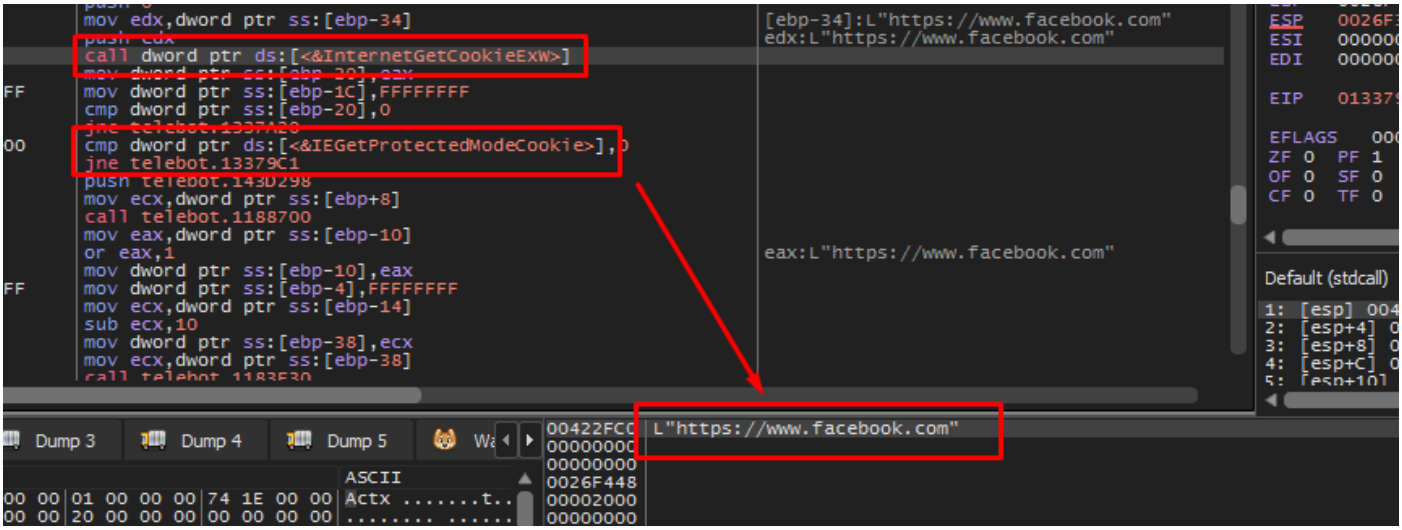
[그림] FFDroider의 감염 및 운영 흐름

[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

FFDroider는 Google Chrome(Chrome 기반 브라우저 포함), Mozilla Firefox, Internet Explorer, Microsoft Edge에 저장된 쿠키 및 계정 크리덴셜을 노립니다.

해당 악성코드는 Chromium SQLite 쿠키를 읽고 파싱하며 Windows Crypt API, 특히 CryptUnProtectData 기능을 악용해 SQLite 크리덴셜 항목을 저장하고 해독합니다.

해당 절차는 InternetGetCookieRxW 및 IEGet ProtectedMode 쿠키와 같은 기능이 Explorer 및 Edge에 저장된 모든 쿠키를 저장하기 위해 사용하는 다른 브라우저와 유사합니다.



[그림] IE에서 Facebook 쿠키를 훔치는 악성코드 기능

[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

탈취 및 암호 해독을 통해 사용자 이름과 패스워드를 일반 텍스트로 생성한 다음 HTTP POST 요청을 통해 C2 서버로 전송됩니다. 이 캠페인에서 C2 주소는 http[:]//152[.]32[.]228[.]19/seemorebty였습니다.

[그림] POST 요청을 통한 도난 데이터 유출

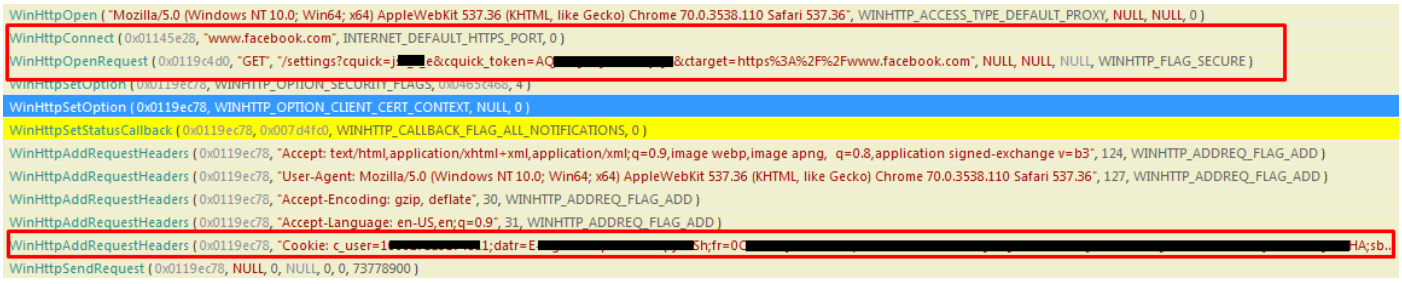
[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

소셜 미디어 계정 노려

다른 많은 패스워드 탈취 트로이 목마와 달리, FFDroider의 운영자는 웹 브라우저에 저장된 모든 크리덴셜을 노리는 것은 아닙니다.

이들은 Facebook, Instagram, Amazon, eBay, Etsy, Twitter, WAX Cloud 지갑 포털을 포함한 소셜 미디어 계정 및 온라인 상점 사이트의 크리덴셜을 훔치는데만 집중합니다.

이들의 목표는 이러한 플랫폼에서 인증하는 데 사용할 수 있는 유효한 쿠키를 훔치는 것이며, 악성코드는 공격 절차 중 즉석에서 해당 계정을 테스트합니다.



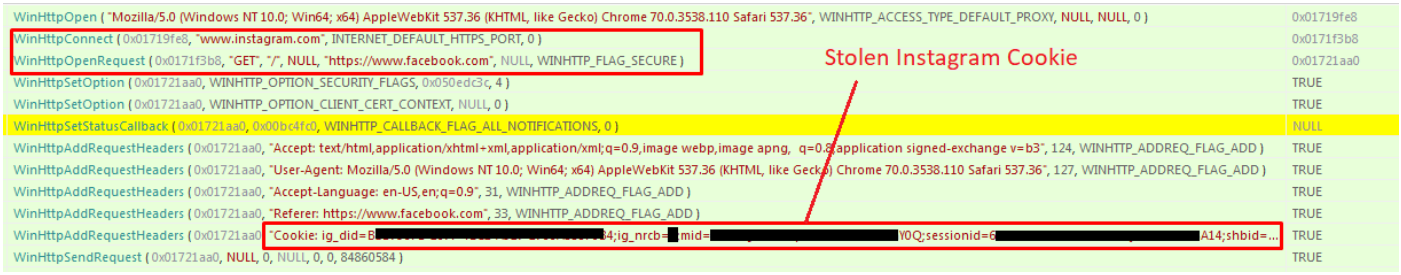
[그림] 브라우저에서 Facebook 쿠키 탈취

[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

예를 들어, Facebook에서 인증이 성공할 경우 FFDroider는 Facebook 광고 관리자에서 모든 Facebook 페이지와 북마크, 피해자의 친구 수, 계정의 청구 및 지불 정보를 가져옵니다.

공격자는 해당 정보를 사용하여 소셜 미디어 플랫폼에서 사기성 광고 캠페인을 실행하고, 더 많은 피해자에게 악성코드를 홍보할 수 있습니다.

공격자가 Instagram 로그인에 성공하면, FFDroider는 계정 편집 웹 페이지를 열어 계정의 이메일 주소, 휴대폰 번호, 사용자 이름, 비밀번호 및 기타 세부 정보를 가져옵니다.



[그림] 훔친 Instagram 쿠키 테스트

[이미지 출처] http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

흥미로운 점은, 이들은 단순히 크리덴셜을 가져오기만 하는 것이 아니라 플랫폼에 로그인하여 더 많은 정보를 훔쳐온다는 것입니다.

이들은 정보를 훔치고 모든 것을 C2로 보낸 후 특정 시간 간격으로 서버에서 추가 모듈을 다운로드합니다.

Zscaler는 해당 모듈에 대한 자세한 정보를 제공하지는 않았지만, 다운로더 기능이 있을 경우 위협은 훨씬 더 강력해집니다.

이러한 악성코드를 예방하려면 불법 다운로드 및 출처를 알 수 없는 소프트웨어를 사용하지 않는 것이 좋습니다.

[출처]
https://www.bleepingcomputer.com/news/security/new-ffdroider-malware-steals-facebook-instagram-twitter-accounts/
http://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

새로운 Meta 인포 스틸러, 악성 스팸 캠페인에서 배포돼

New Meta information stealer distributed in malspam campaign

최신 악성 스팸 캠페인이 사이버 공격자 사이에서 인기있는 인포 스틸러 악성코드인 새로운 META 악성코드를 배포하는 것으로 나타났습니다.

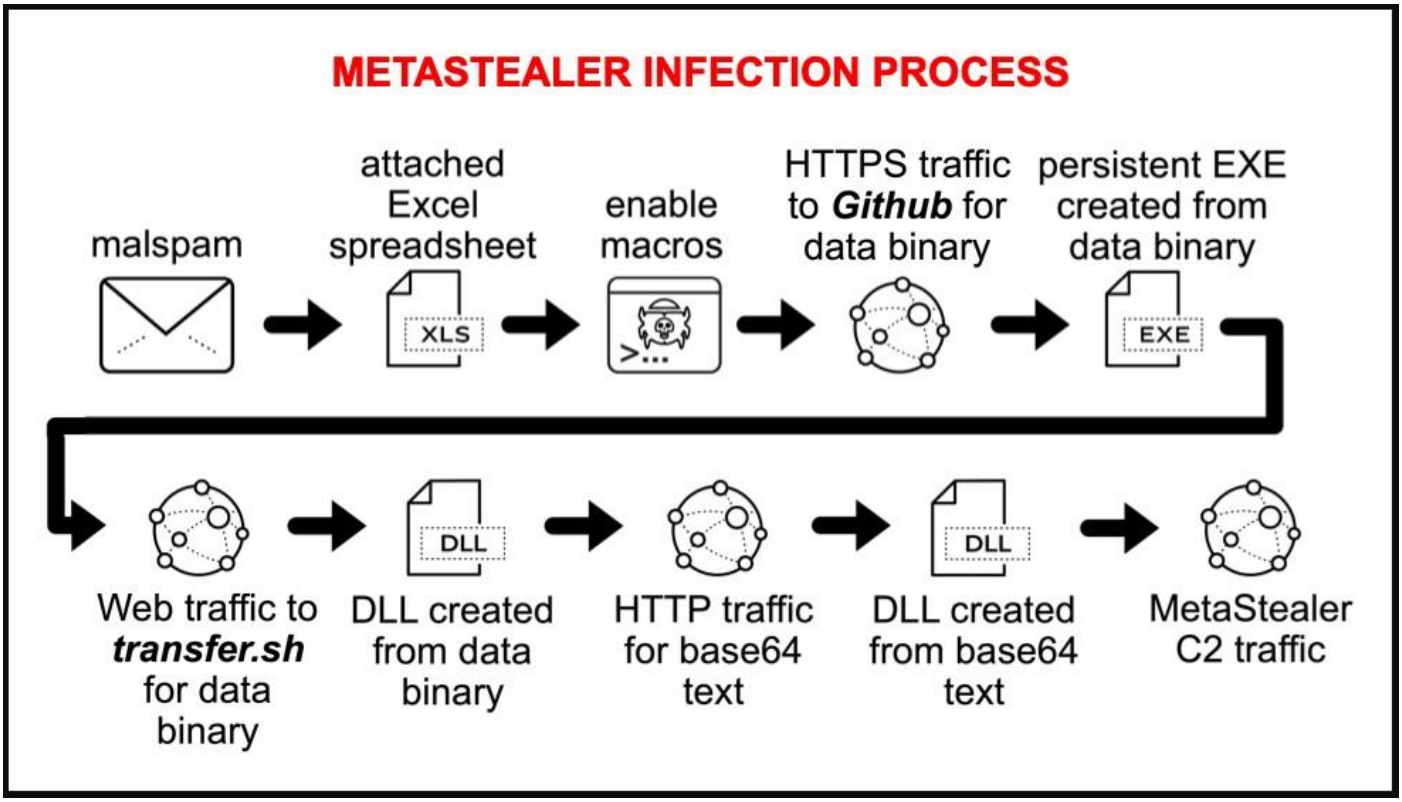
META는 Mars Stealer, BlackGuard와 함께 새로운 인포 스틸러 중 하나로, 운영자는 Raccoon Stealer가 운영을 중단한 후 다른 플랫폼을 찾고 있는 사람들을 이용합니다.

이 툴은 한 달에 $125, 무제한 $1,000에 판매되고 있으며 RedLine의 개선된 버전이라 광고했습니다.

새로운 Meta 악성 스팸 캠페인

보안 연구원인 Brad Duncan이 발견한 이 새로운 스팸 캠페인은 META가 공격에 적극적으로 사용되어 Chrome, Edge, Firefox에 저장된 비밀번호와 가상화폐 지갑을 훔치는 데 사용된다는 것을 알 수 있는 증거가 됩니다.

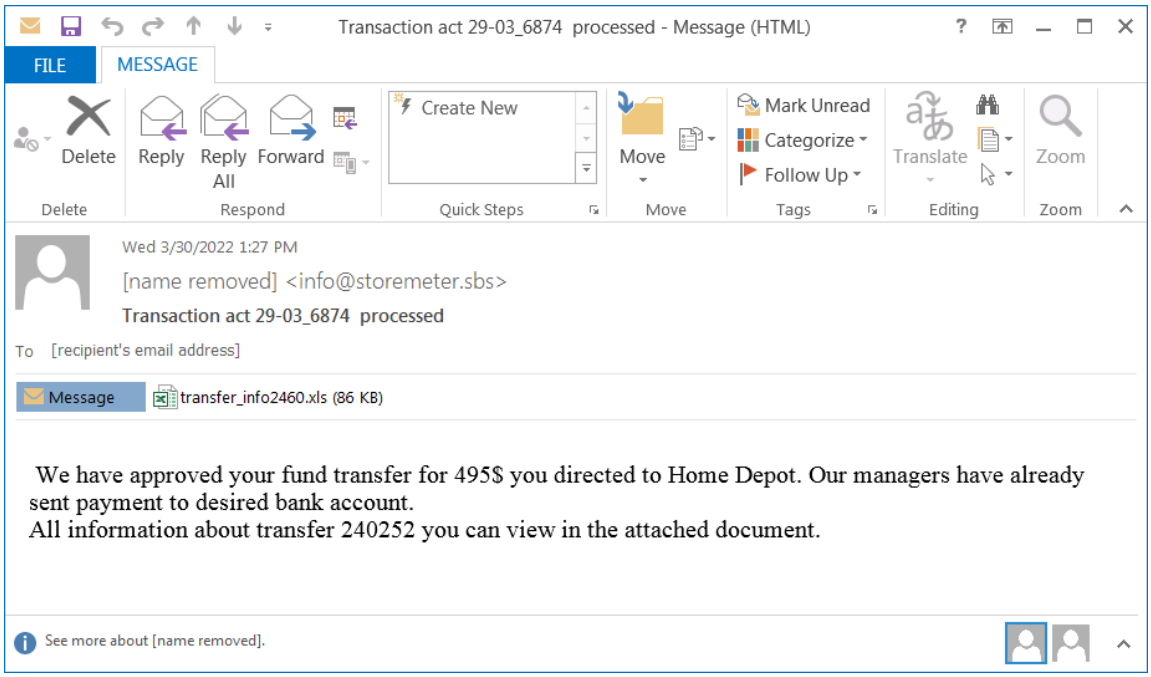
이 특정 캠페인의 감염 체인은 이메일 첨부 파일로 시작되며, 매크로가 활성화된 엑셀 스프레드 시트를 사용합니다.



[그림] 발견된 캠페인의 META 감염 체인

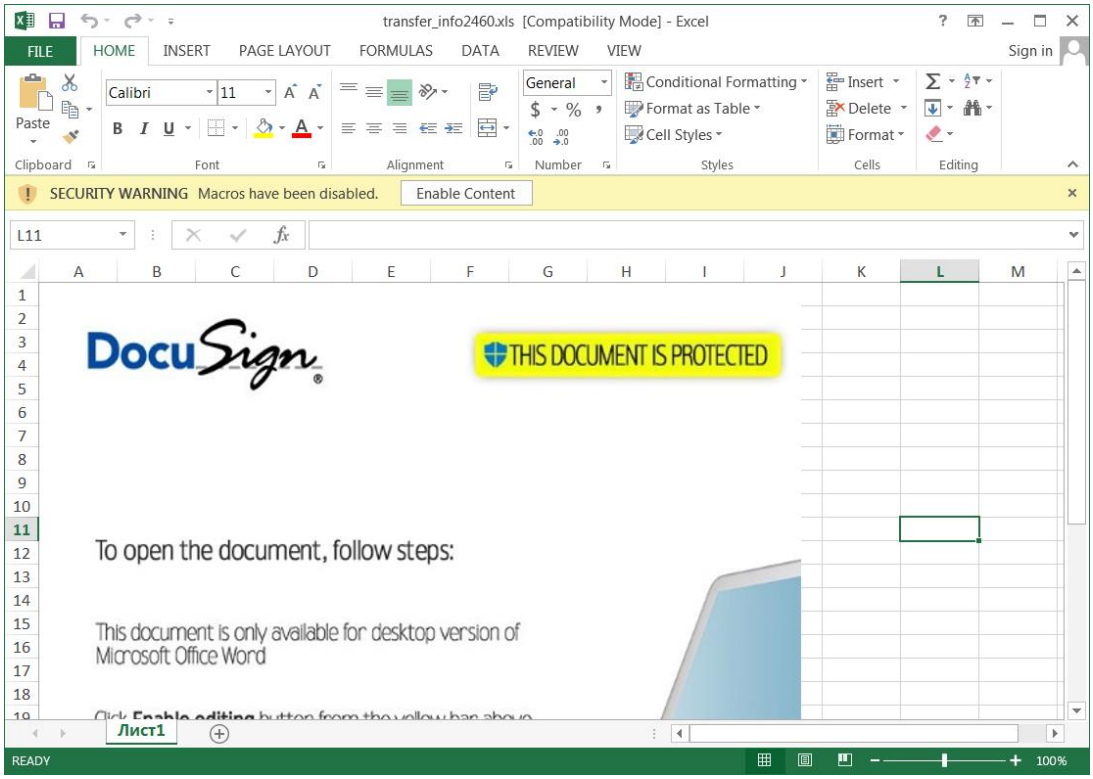
[이미지 출처] https://isc.sans.edu/

메시지는 딱히 설득력이 있지 않고 잘 작성된 것은 아니지만, 여전히 많은 수신자가 속을 수 있는 자금 이체 관련 미끼를 사용합니다.



[그림] 악성 엑셀 첨부 파일이 포함된 이메일
[이미지 출처] https://isc.sans.edu/

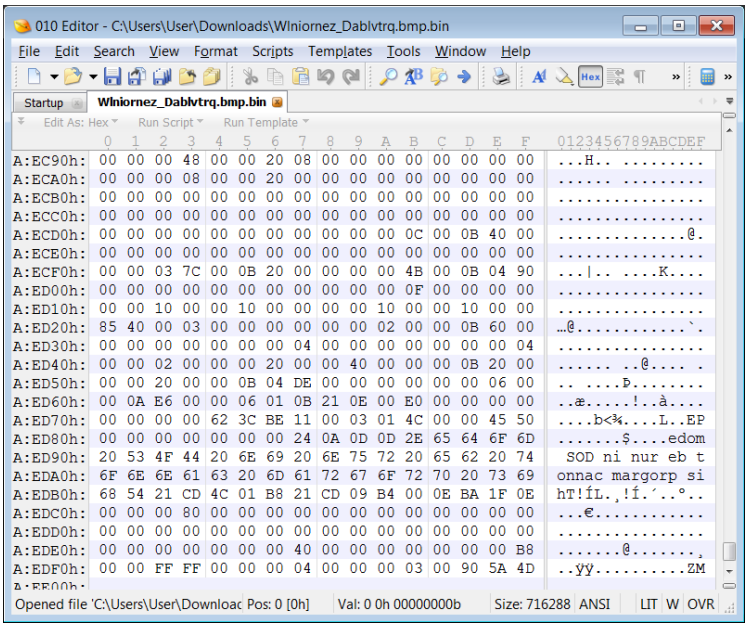
스프레드시트 파일은 백그라운드에서 악성 VBS 매크로를 실행할 수 있도록 "콘텐츠를 활성화"하도록 속이기 위해 DocuSign 관련 미끼를 사용합니다.



[그림] 사용자가 콘텐츠를 활성화하도록 유도하는 DocuSign 미끼
[이미지 출처] https://isc.sans.edu/

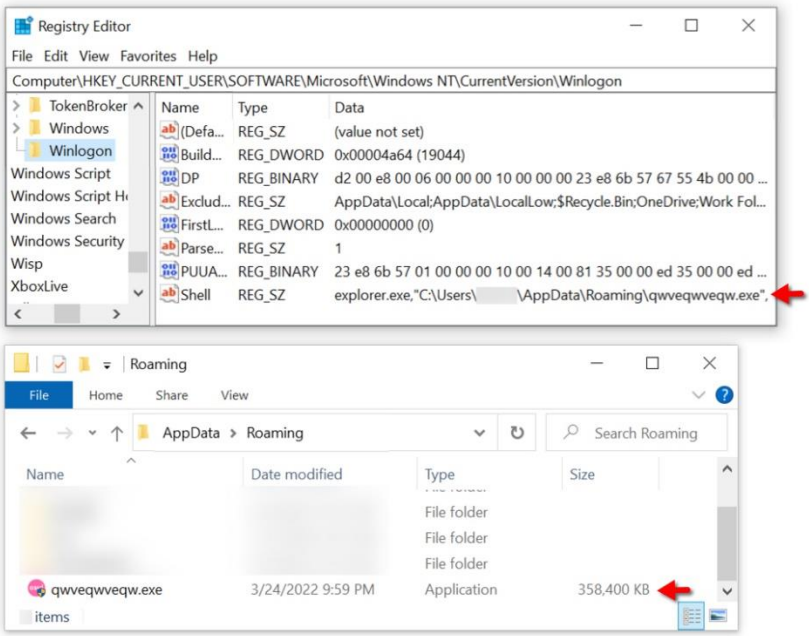
악성 스크립트가 실행되면 GitHub을 포함한 사이트 다수에서 DLL 및 실행 파일을 포함한 다양한 페이로드를 다운로드합니다.

다운로드한 파일 중 일부는 base64로 인코딩되어 있거나 보안 소프트웨어의 탐지를 우회하기 위해 바이트가 반전되어 있습니다. 예를 들어 아래는 원본 다운로드에서 바이트가 반전된 샘플 중 하나입니다.



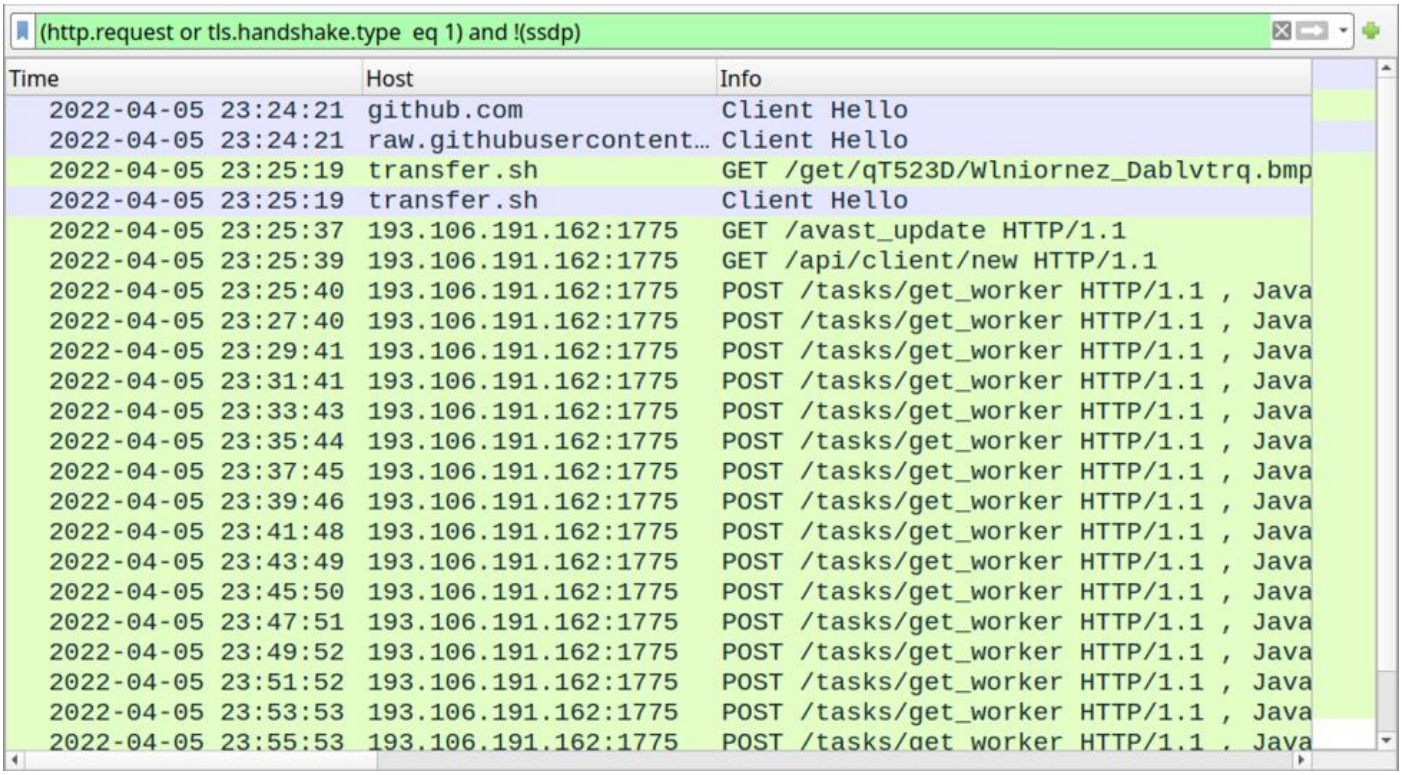
[그림] 역 바이트 순서로 저장된 DLL
[이미지 출처] https://isc.sans.edu/

최종 페이로드는 랜덤으로 생성되었을 가능성이 있는 "qwveqwveqw.exe"라는 이름으로 컴퓨터에서 어셈블되며 지속성을 얻기 위해 새 레지스트리 키를 추가합니다.



[그림] 새 레지스트리 키 및 악성 실행 파일
[이미지 출처] https://isc.sans.edu/

시스템이 감염되었음을 확인할 수 있는 명확 징후는 193.106.191[.]162에 있는 명령 및 제어 서버로 트래픽을 생성하는 EXE 파일이며, 이는 시스템이 재부팅된 후에도 감염된 시스템에서 감염 프로세스를 다시 시작합니다.


(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Host	Info
2022-04-05 23:24:21	github.com	Client Hello
2022-04-05 23:24:21	raw.githubusercontent…	Client Hello
2022-04-05 23:25:19	transfer.sh	GET /get/qT523D/Wlniornez_Dablvtrq.bmp
2022-04-05 23:25:19	transfer.sh	Client Hello
2022-04-05 23:25:37	193.106.191.162:1775	GET /avast_update HTTP/1.1
2022-04-05 23:25:39	193.106.191.162:1775	GET /api/client/new HTTP/1.1
2022-04-05 23:25:40	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:27:40	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:29:41	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:31:41	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:33:43	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:35:44	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:37:45	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:39:46	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:41:48	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:43:49	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:45:50	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:47:51	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:49:52	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:51:52	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:53:53	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java
2022-04-05 23:55:53	193.106.191.162:1775	POST /tasks/get_worker HTTP/1.1 , Java

[그림] Wireshark에서 캡처된 악성 트래픽
[이미지 출처] https://isc.sans.edu/

한 가지 주목 할 점은, META가 PowerShell을 통해 Windows Defender를 수정하여 .exe 파일을 검색에서 제외하고 해당 파일이 검색되지 않도록 보호한다는 것입니다.

[출처]
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://www.malware-traffic-analysis.net/2022/04/06/index.html (IOC)

www.estsecurity.com

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616