이스트시큐리티

보안 동향 보고서

No.140 2021.05

No.140 2021.05

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 4 월에도 국내외 다양한 조직들을 타깃으로 한 지속적인 APT 공격이 다수 포착되었습니다.

특히 외교·안보·국방·통일 분야에 종사하는 전문가나 관계자를 겨냥한 이메일 해킹 시도가 국내에서 지속되고 있습니다. 해당 공격의 배후로는 오래 전부터 북한 당국과 연계된 것으로 공식적으로 언급되어 온 탈륨(Thallium)과 라자루스(Lazarus) 조직이 지목됐습니다. 이들의 공격은 악성 DOC 문서를 이메일에 첨부하여 보내는 전통적인 피싱 방식이 주를 이루지만 수신자를 현혹시키기 위한 위협 시나리오가 나날이 정교해지고 있어 각별한 주의가 필요합니다. 또한 각 조직은 국내 특정 분야를 대상으로 은밀하게 사이버 위협 행위에 가담하고 있어 그 이면에 어떤 목적을 가지고 있는지 특정짓기 어렵기 때문에 각 조직에서는 위협에 노출되지 않도록 해야 합니다.

더불어 전 세계적으로 암호화폐 거래가 성행함에 따라 국내에서도 가상 자산 플랫폼 '빗썸'의 계정 탈취를 목적으로 발송된 피싱 메일이 발견됐습니다. 이번에 발견된 피싱 메일은 '계정 정지'를 주제로 사용자에게 계정 정보를 확인하지 않으면 계정이 정지될 수 있다는 문구로 사용자의 클릭을 유도했습니다. 사용자가 피싱 사이트에 계정 정보를 입력하게 되면, 계정, 비밀번호 뿐만 아니라 접속한 IP 주소, 국가 정보, 도시 등 whois 정보 전체가 전달되며, 탈취된 정보는 향후 공격자들의 또다른 악성 캠페인에 악용될 가능성이 큽니다. 암호화폐 관련 피싱 메일은 지속적으로 발견되고 있으므로, 사용자는 관련 메일 수신 시 발신자의 주소 및 첨부된 링크의 도메인 주소를 꼼꼼히 살피는 습관을 갖는 것이 좋습니다.

이스트시큐리티에서는 4 월에 2021 년 1 분기 알약 랜섬웨어 행위 기반 차단 통계를 발표했습니다. 2021 년 1 분기 동안 알약을 통해 총 154,887 건의 랜섬웨어 행위기반 공격이 차단된 것으로 확인됐습니다. 통계는 개인 사용자를 대상으로 무료 제공하는 공개용 알약의 '랜섬웨어 행위 기반 차단 기능'을 통해 차단된 공격만을 집계한 결과로, 패턴 기반 탐지건까지 포함한다면 전체 공격을 더욱 많을 것으로 예상됩니다.

랜섬웨어 공격자들은 더 많은 수익을 창출하기 위해 랜섬머니를 갈취할 다양한 방법을 고안하고 있습니다. DoppelPaymer 랜섬웨어 운영 그룹은 그들의 다크웹에 현대기아차를 비롯한 계열사 데이터를 게시한 바가 있으며 지난해 말 CLOP 랜섬웨어 조직이 이랜드 그룹을 감염시키고 탈취한 카드정보를 비롯한 데이터를 공개한 사례도 있습니다. 특히나 올해 첫 기업용 랜섬웨어로 공개됐던 Babuk 랜섬웨어의 경우 감염된 시스템을 암호화하지 않고 데이터만 훔친 뒤 유출하는 데이터 강탈 랜섬웨어로 사업 모델을 변경하겠다고 밝혀 향후 더 많은 기업들이 피해를 입을 가능성이 대두됐습니다.

최근 공격자들은 지속적으로 공격 기능을 고도화하고 공격 범위를 확대해 가는 모습을 보여주고 있습니다. 따라서 기업 관계자를 비롯한 모든 사용자는 항상 컴퓨터 및 인터넷 사용 습관에 주의해야 하며 사이버 보안에 관심을 갖는

01 악성코드 통계 및 분석

자세가 필요합니다. 또한 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 4 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Hosts.media.opencandy.com 와 Misc.HackTool.AutoKMS 이 각각 1 위와 2 위를 차지했으며 Trojan.Agent.Injector.Gen 을 비롯한 5 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 눈에 띄는 부분으로는 Misc.Riskware.Segurazo 와 JS:Trojan.Cryxos.5275 가 지난달 순위에서 6 계단씩 하락하여 13 위와 15 위를 차지했으며, 그 외에는 큰 순위 변동 없이 대체적으로 지난달과 유사한 순위 양상을 보였다.

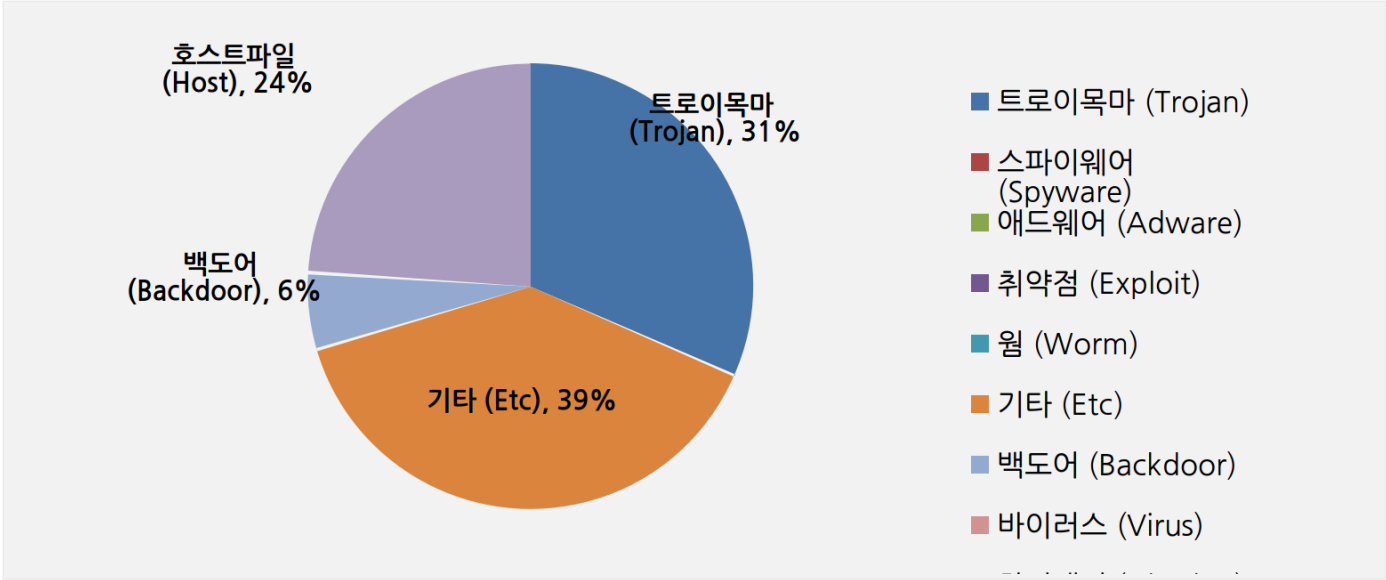
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	696,093
2	-	Misc.HackTool.AutoKMS	ETC	346,505
3	-	Trojan.ShadowBrokers.A	Trojan	289,479
4	New	Trojan.Agent.Injector.Gen	Trojan	179,792
5	↓1	Misc.HackTool.KMSActivator	ETC	168,075
6	New	Misc.Riskware.BitCoinMiner	ETC	164,259
7	↓1	Backdoor.Generic.792814	Backdoor	159,909
8	New	Trojan.GenericKD.46161563	Trojan	143,373
9	New	Gen:Variant.Razy.715313	ETC	137,128
10	New	JS:Trojan.Cryxos.5175	Trojan	121,395
11	↓3	Misc.Keygen	ETC	109,339
12	↓1	Misc.Riskware.TunMirror	ETC	98,762
13	↓6	Misc.Riskware.Segurazo	ETC	97,700
14	↓4	Trojan.Agent.Gen	Trojan	91,836
15	↓6	JS:Trojan.Cryxos.5275	Trojan	81,223

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 04 월 01 일 ~ 2021 년 04 월 30 일

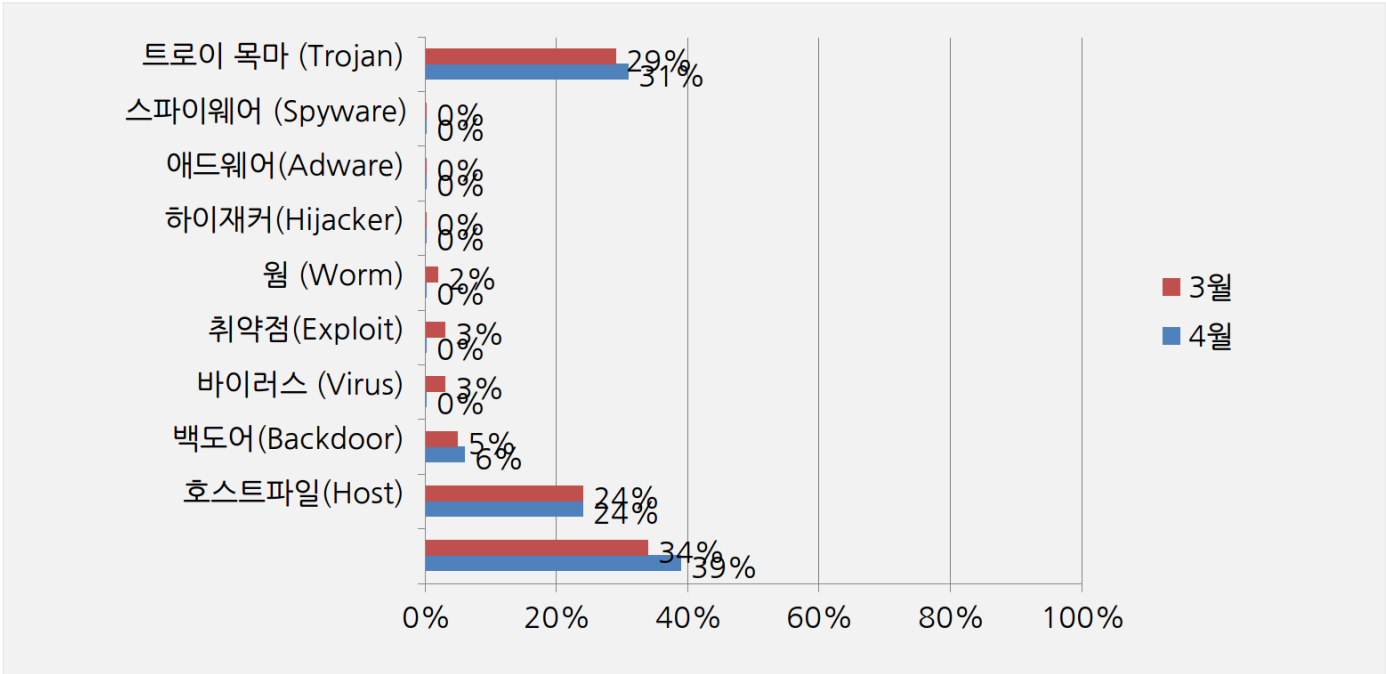
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 39%를 차지했으며 트로이목마(Trojan) 유형이 31%로 그 뒤를 이었다. 지난달 기타 유형을 제외하고 두 번째로 많은 비중을 차지했던 호스트파일(Host) 유형이 24%로 지난달과 동일한 수치를 기록했으며, 지난달 5%를 차지했던 백도어(Backdoor) 악성코드 유형이 소폭 증가하여 6%를 기록했다. 2021 년 3 월과 비교하여 전체 감염 건수는 약 1.32% 증가하였다 .



카테고리별 악성코드 비율 전월 비교

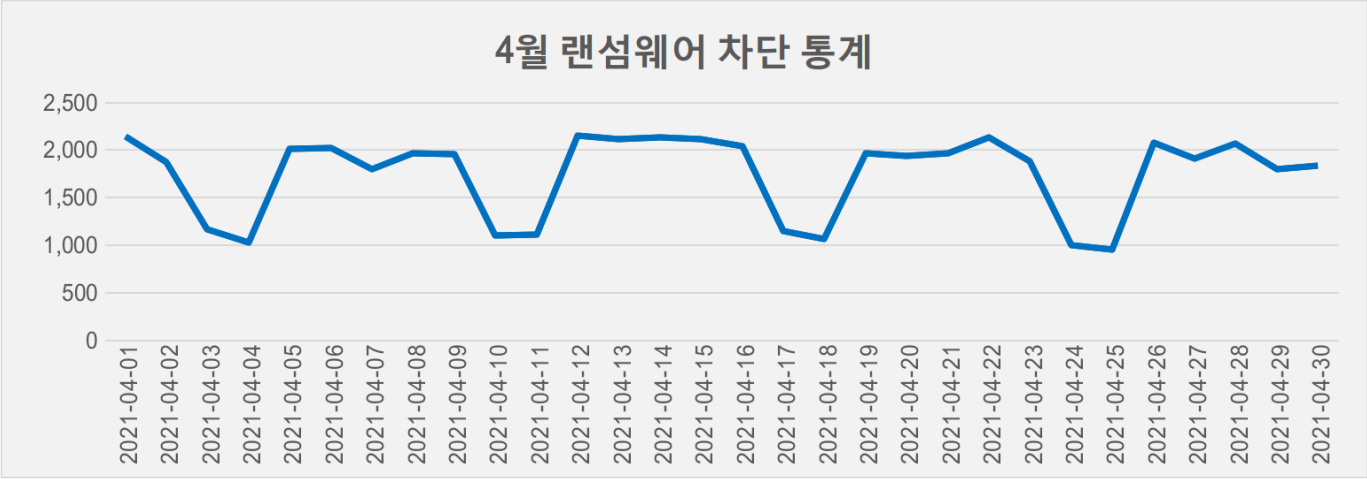
4 월에는 지난 3 월과 비교하여 트로이목마(Trojan) 유형이 2% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 동일한 수치를 기록했다. 또한 지난달 탐지됐던 웜(Worm), 바이러스(Virus), 취약점(Exploit) 유형의 수치가 감소하여 악성코드 탐지율 Top 15 에 기록되지 못했다. 3 월에 5%를 차지했던 백도어(Backdoor) 유형이 소폭 증가하여 6%를 기록했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

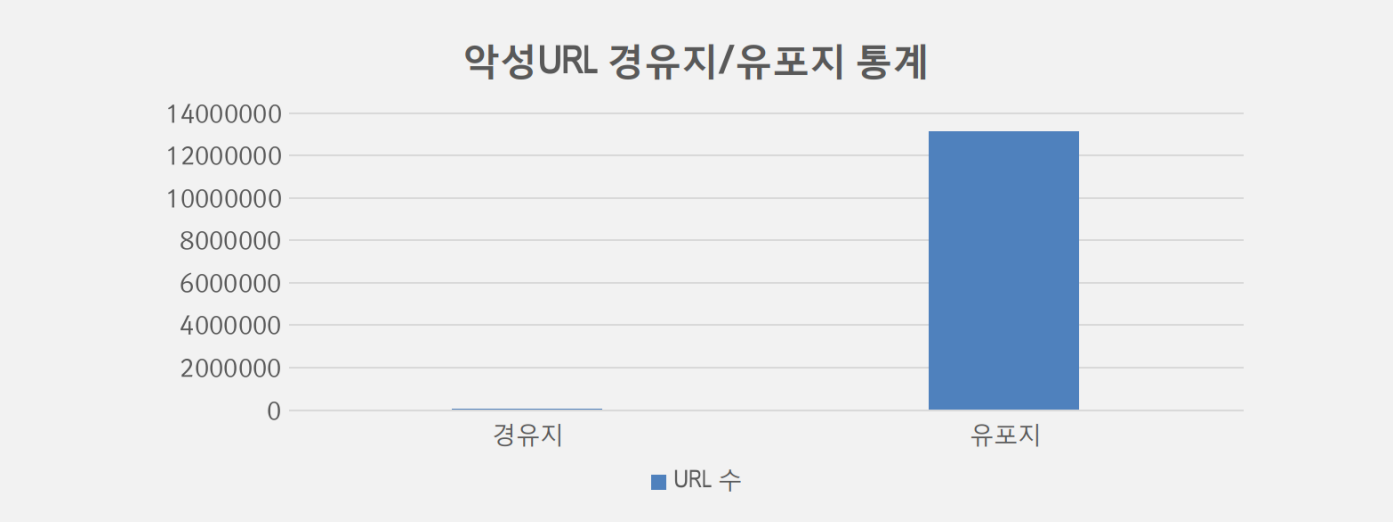
4 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 4 월 1 일부터 4 월 30 일까지 총 52,742 건의 랜섬웨어 공격 시도가 차단되었다. 3 월의 랜섬웨어 공격 건수인 54,250 건에 비해 약 2.78% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 4 월 한 달간 총 6,585,240 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 3 월 한 달간 확인되었던 13,167,607 건의 악성코드 경유지/유포지 URL 수에 비해 약 49.99% 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

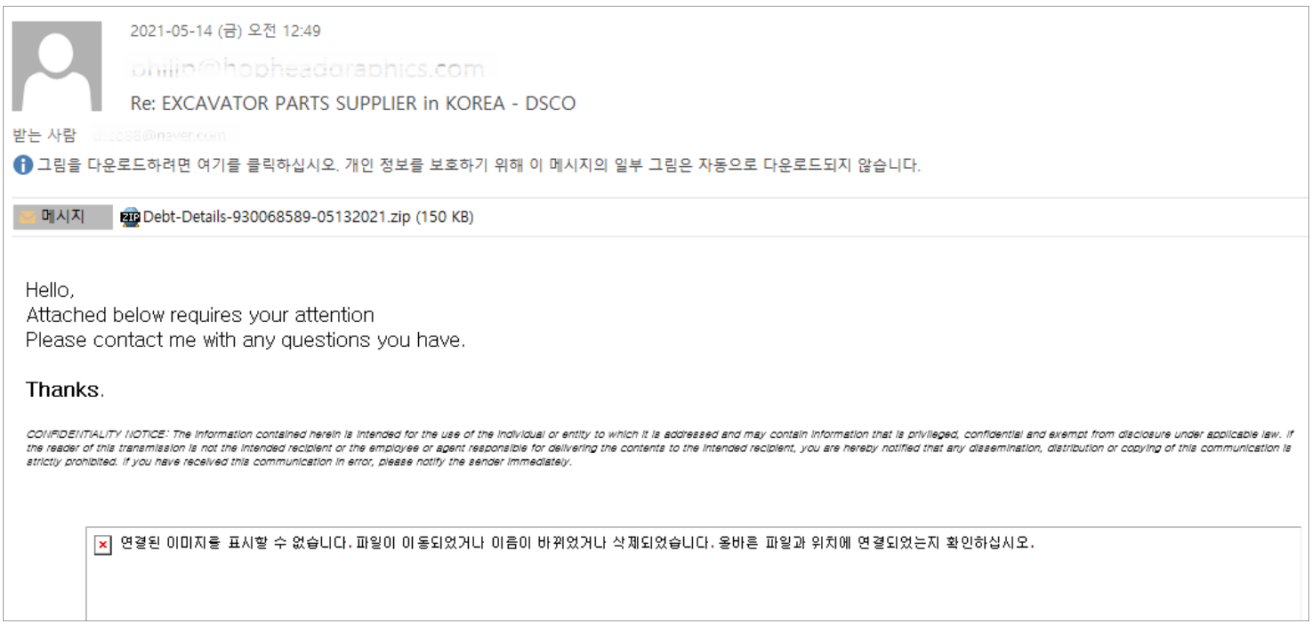
1. 장학금 신청 관련 내용으로 유포중인 Qbot 악성코드 발견!
2. ′북한비핵화′ 관련 내용 담은 악성문서 유포

1. 장학금 신청 관련 내용으로 유포중인 Qbot 악성코드 발견!

최근 국내 유명 대학교 교직원 장학금 신청 관련 내용으로 피싱 메일이 다량 유포되고 있어 관련자들의 각별한 주의가 필요합니다.

[그림 1-1] 장학금 신청 관련 내용으로 위장한 피싱 메일

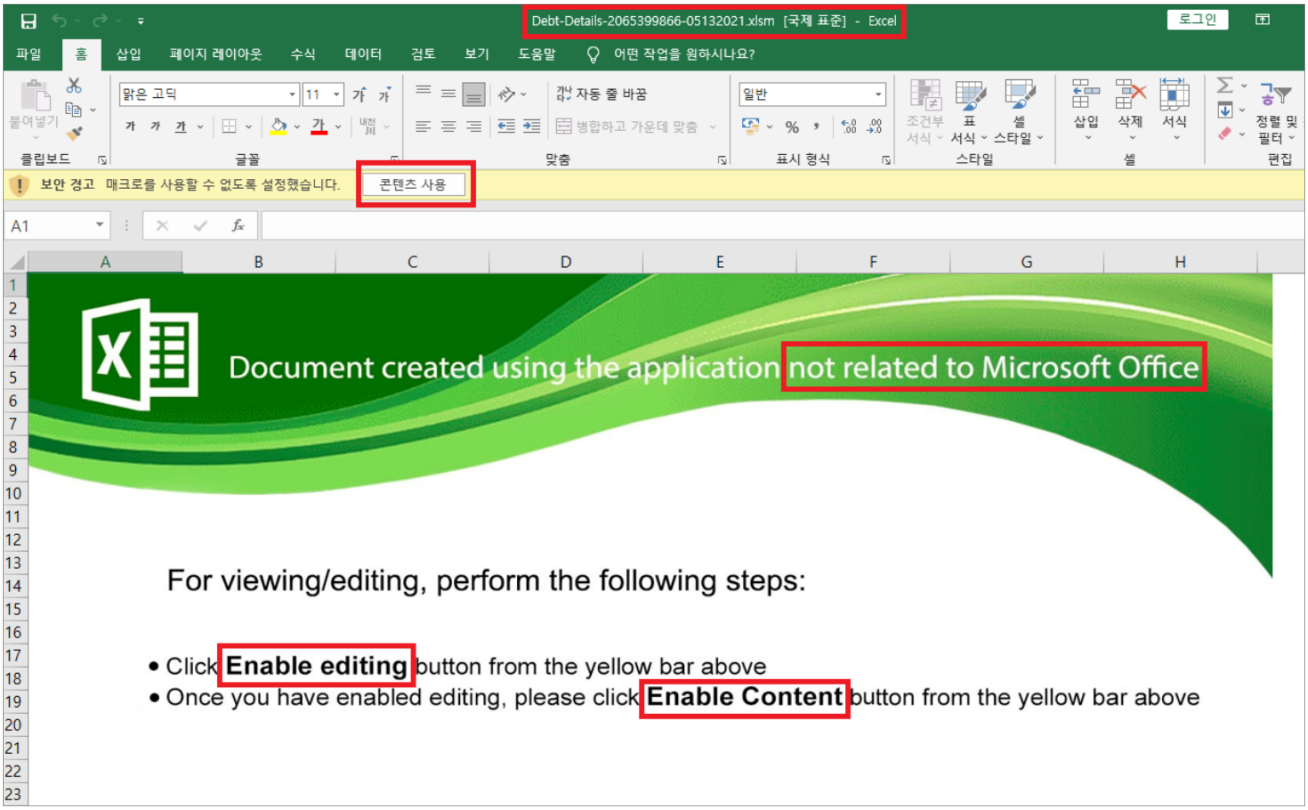
5 월 13 일 오후 11 시 43 분 경에 수신된 것으로 확인되는 메일들은 'Re: 00 대학교 교직원 장학금 장학생 모집 신청서 예술공학부', 'Re: 00 대학교 교직원 장학금 신청서 (20163100 김한빈)', 'Re: 00 대학교 교직원 장학금 신청서 -20196231 양란아'와 같은 제목을 사용하며, 본문에는 학생의 이름, 전공과 학번 등을 포함해 장학금을 신청한다는 내용을 담고 있습니다. 본문은 영어와 한글 버전이 모두 작성되어 있어, 수신자의 국적에 관계 없이 첨부파일을 열어보도록 유도했습니다. 메일에 사용된 발신 주소 도메인은 실제로 존재하는 스페인, 캐나다 등의 해외 기업으로 신뢰성을 높였습니다. 수신자 도메인은 모두 국내 유명 포털사이트 계정을 사용했습니다.



[그림 1-2]5 월 14 일 추가 발견된 피싱 메일

02 전문가 기고

금일(5 월 14 일) 오전 12 시 49 분 경, 'Re: EXCAVATOR PARTS SUPPLIER in KOREA – DSCO'라는 제목의 피싱 메일이 추가로 발견되었습니다. 발신 주소 역시 실제 존재하는 웹 디자인 기업이며, 수신자 도메인 또한 위 3 개의 메일과 동일하게 국내 유명 포털사이트 계정을 사용했습니다.

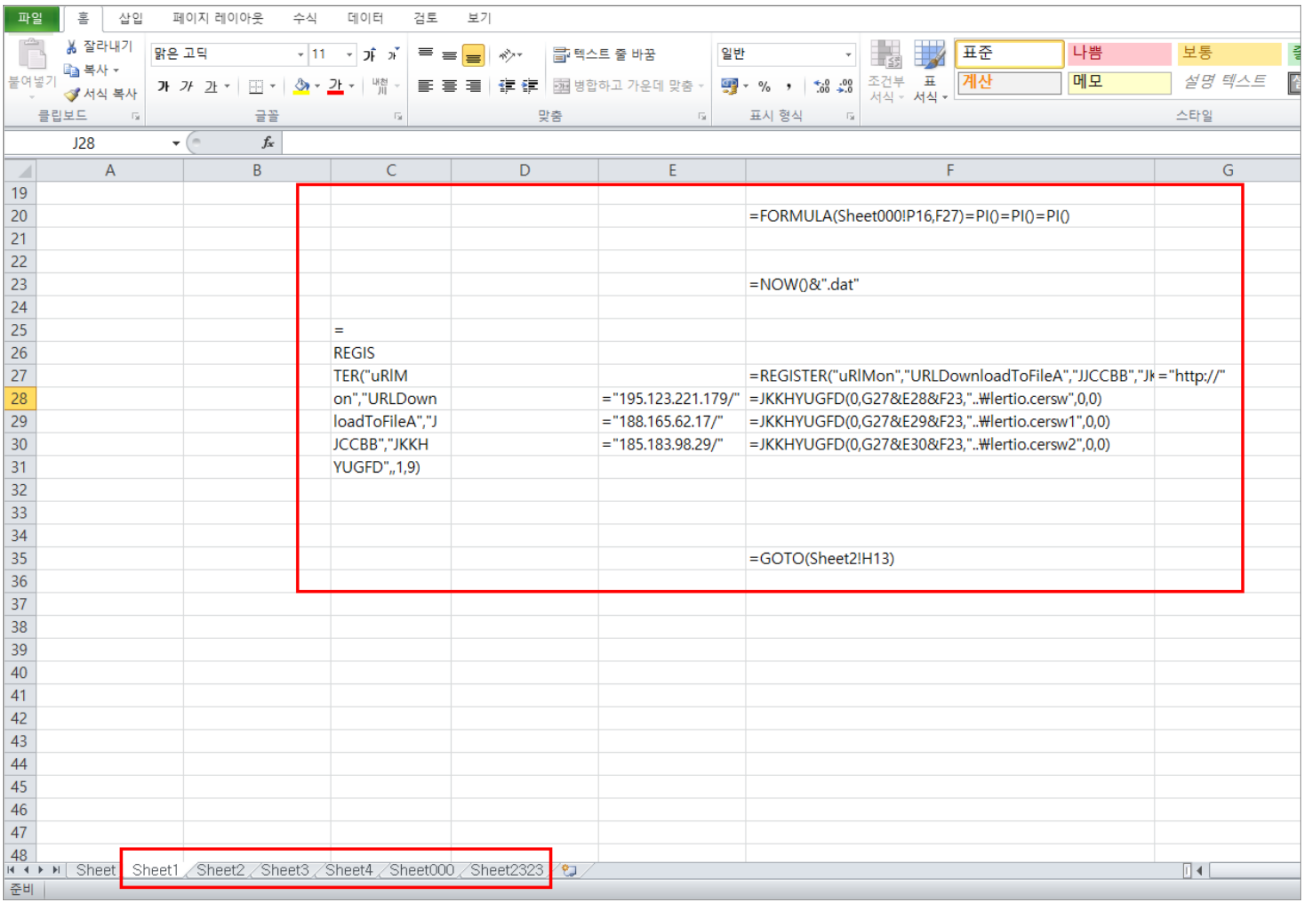


[그림 2] 첨부파일 내 포함된 엑셀 파일

발견된 4 개의 메일에는 공통적으로 zip 압축 파일이 포함되어 있습니다. 해당 파일들은 'Debt-Details-2065399866-05132021.zip', 'Debt-Details-2037842254-05132021.zip', 'Debt-Details-1184647712-05132021.zip', 'Debt-Details-930068589-05132021.zip' 파일명을 사용하며, 압축 파일 내에는 확장자만 변경된 액셀(xlsm) 파일이 포함되어 있습니다.

해당 파일 실행시, 문서 상단에는 '매크로를 사용할 수 없도록 설정했습니다.'라는 문구를 포함한 보안 경고창이 나타나며, 문서 열람 및 편집을 위해 사용자에게 '편집 사용' 버튼 및 '콘텐츠 사용' 버튼을 클릭하도록 유도합니다.

해당 내용은 영문으로 작성되어 있으며, 'Microsoft Office 과 관련 없는' 애플리케이션을 사용하여 제작된 문서라는 내용이 본문 상단에 나타납니다.



[그림 3] 엑셀 파일에 숨겨진 시트와 매크로 구문

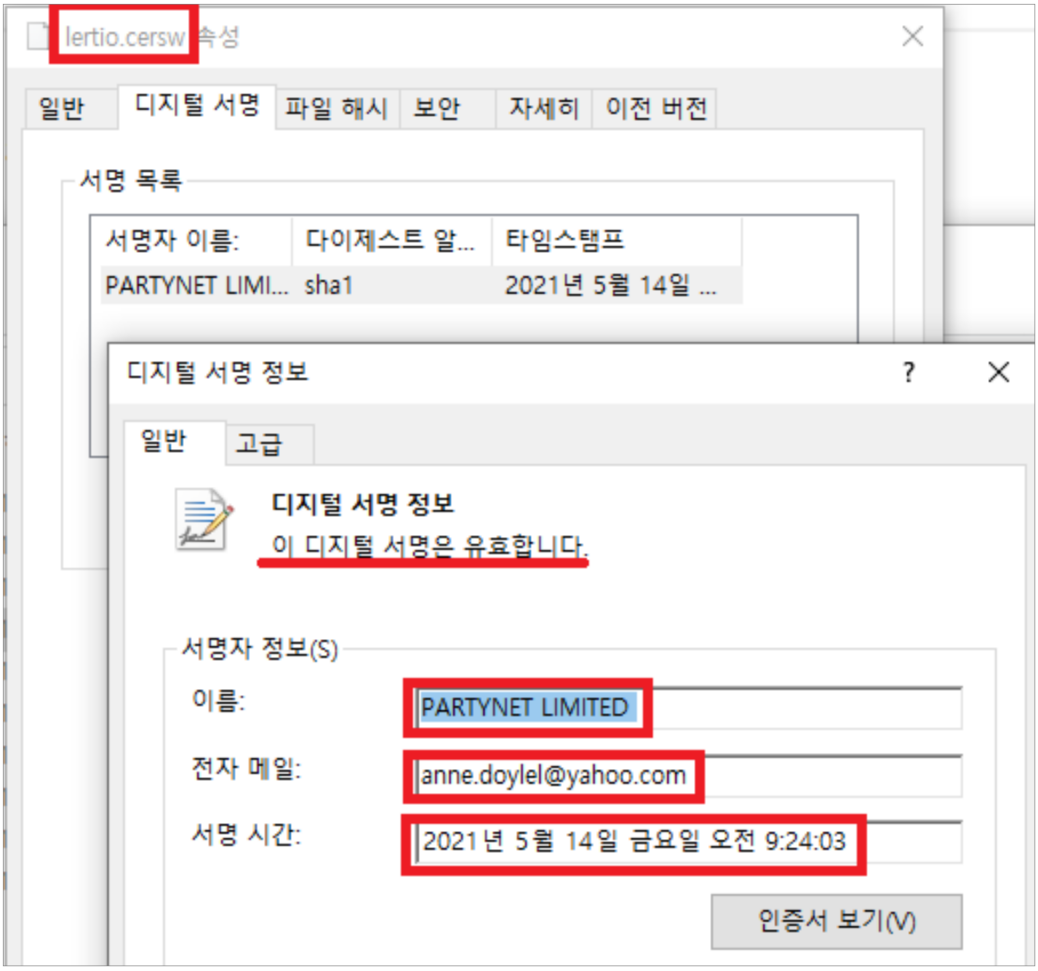
엑셀 파일은 위 그림과 같이 총 6 개의 숨겨진 Sheet 가 존재하며 각 Sheet 마다 매크로 구문이 작성되어 있습니다.

매크로 동작 시 문서 내에 기재 된 C2 서버를 사용하여 아래 URL 에서 동일한 파일 (lertio.cersw, lertio.cersw1, lertio.cersw2)들을 다운로드 받습니다.

* 발견된 4 개 메일의 첨부파일 모두 동일한 C2 서버를 사용합니다.

다운로드 형태는 'hxxp://c2 서버/[=NOW()]&".dat'로, 분석 당시 아래 주소가 확인되었습니다.

hxxp://195.123.221.179/44330.4968458333.dat (lertio.cersw)
hxxp://188.165.62.17/44330.4968458333.dat (lertio.cersw1)
hxxp://185.183.98.29/44330.4968458333.dat (lertio.cersw2)



[그림 4] 유효한 디지털 서명이 사용된 화면

lertio.cersw 속성을 살펴보면, 유효한 디지털 서명이 사용된 것을 볼 수 있습니다. 'PARTYNET LIMITED'라는 이름과 'anne.doylel@yahoo.com' 도메인을 사용했고, 서명 시간은 2021 년 5 월 14 일 금요일 오전 9 시 24 분 경으로 나타납니다. 또한 Process 생성, Mutex 생성, Process 인젝션, Directory 생성, File 생성/복사/이름 변경, File, Directory 속성 변경, Registry 생성, Registry 값 설정, Network 접속 등의 동작을 실행합니다.

확인 결과, 해당 파일은 QakBot(이하 Qbot) 악성코드로 확인되었습니다. 'QBot'는 사용자 PC 정보를 수집 및 전송 후 C&C 에서 공격자 명령에 따라 다운로더, 인젝션 등 추가 악성 행위를 수행하는 악성코드입니다. 특징적으로 주목할 만한 기능에는 백신 프로세스에 따라 악성코드 설치 및 실행 방법이 다르며, 페이로드에서 약 151 개의 C&C 목록을 사용한다는 점이 있습니다. 또한 C&C 에서 브라우저, 뱅킹 정보 탈취 관련 추가 모듈 등을 다운받는 것으로 알려져 있어, 특히 기업체에서 감염이 되는 경우 큰 피해가 발생할 가능성이 높습니다.

따라서 악성코드로부터 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일에 접근하지 않도록 주의해야 합니다.

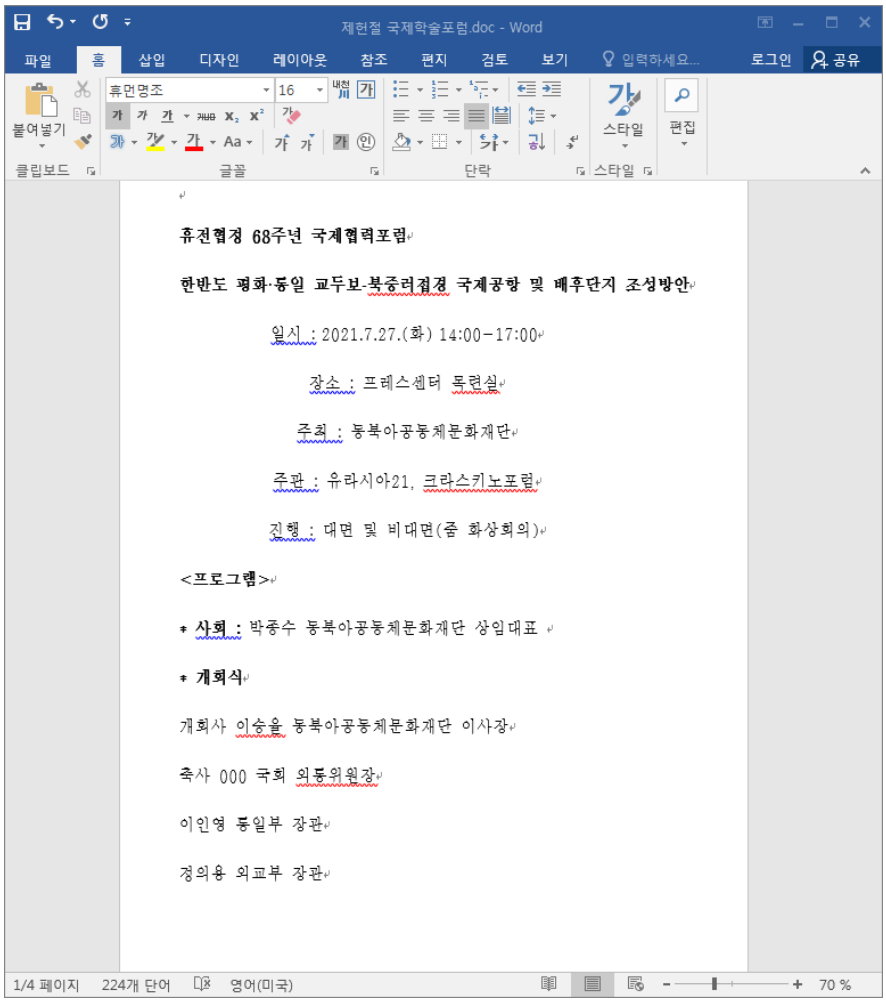
현재 알약에서는 해당 악성 코드를 'Trojan.Downloader.XLS.gen', 'Trojan.Agent.QakBot' 탐지 명으로 진단하고 있으며, 관련 IoC 및 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능합니다 .

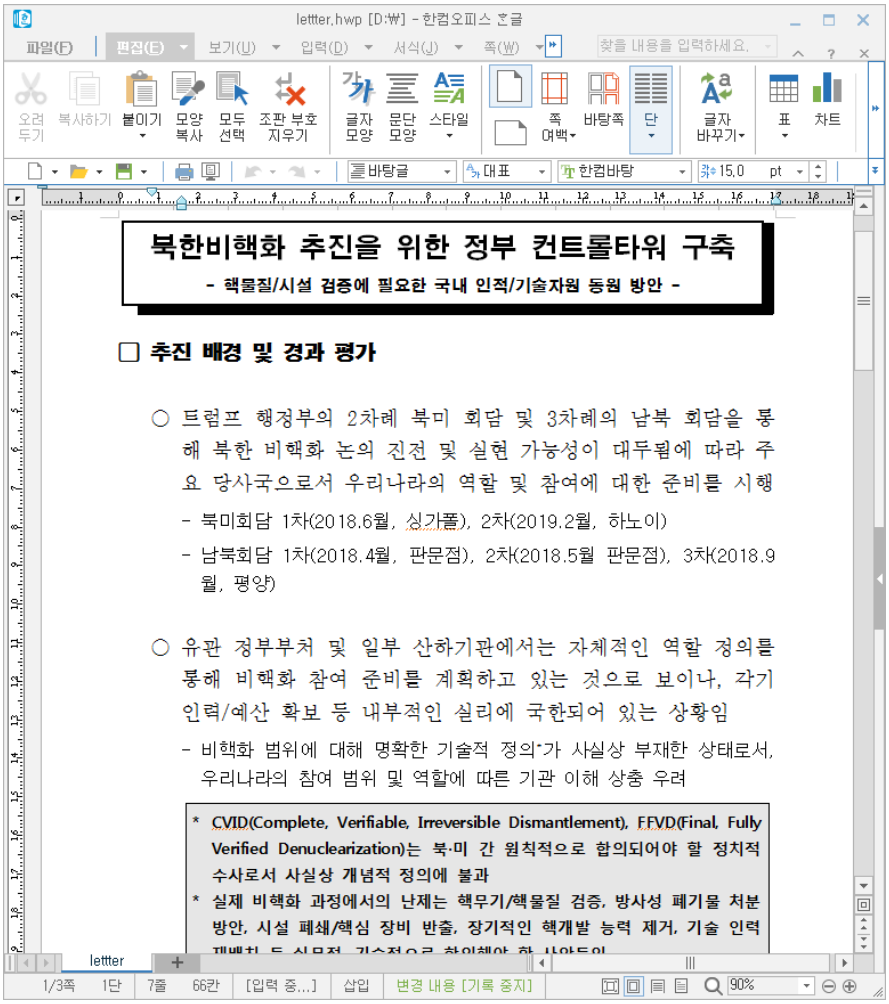
2. ‘북한비핵화’ 관련 내용 담은 악성문서 유포

오는 21 일 열리는 한미정상회담을 계기로 북미대화 재개 가능성이 조심스럽게 나오는 가운데, 북한 배후 해킹 그룹 ‘탈륨(Thallium)’이 활발하게 활동중인 정황이 발견돼 대북 관련 전문가와 관계자의 각별한 주의가 요구됩니다.

최근 탈륨 조직의 ‘제헌절 국제학술포럼’, ‘북한비핵화컨트롤타워구축(안)’ 등으로 위장한 피싱 공격이 탐지되었습니다.

제헌절 국제학술포럼은 7 월 27 일 진행 일정의 포럼 내용을 담고 있으며, 개회식 내용에 통일부와 외교부장관 이름이 포함돼 있고, ‘한반도 평화·통일 교두보–북중러접경 국제공항 및 배후단지 조성방안’이라는 내용이 담겨 있습니다.





[그림] 11 일과 12 일 연속으로 발생한 탈륨의 공격 캠페인

이러한 유형은 신뢰할만한 문서 내용처럼 수신자를 현혹하는 전형적인 스피어피싱 공격으로, '북한비핵화컨트롤타워 구축(안)'이라는 제목의 문서는 '핵물질·시설 검증에 필요한 국내 인적·기술자원 동원 방안'이라는 제목으로, 관련 산하기관으로 산업자원부, 과기정통부, 국방부, 원자력안전위원회 등의 내용이 포함돼 있습니다.

탈륨은 우리나라에서 3 가지 중요한 APT 캠페인을 벌이고 있으며, ▲대북 언론기자와 북한 인권 분야 활동 관계자를 노리는 스모크 스크린(Smoke Screen) ▲국내외 방위산업체, 비트코인 거래소, 코로나 19 관련 제약회사, 교육연구분야 등을 타깃으로 하는 블루 에스티메이트(Blue Estimate) ▲대북단체, 외교·안보·국방·통일분야 전문가를 주요 표적으로 삼는 페이크 스트라이커(Fake Striker)로 구분됩니다. 모든 캠페인에서 북한분야 연구 및 활동가들이 모두 위협 대상에 포함됩니다.

이들은 북한식 언어 스타일과 폰트(천리마체), 이름(리영민) 등을 사용한 것이 포착된 바 있고, 스피어피싱과 공급망 공격을 함께 쓰며, 윈도우 운영체제 뿐만 아니라 안드로이드와 맥용 악성 파일을 유포한 이력도 발견됐습니다. 전문가들은 탈륨 조직의 정교하고 고도화된 사이버 위협 활동이 증가하고 있어 피해 가능 우려가 높아지고 있다고 경고합니다.

02 전문가 기고

이들은 주로 이메일 기반의 해킹 공격을 주무기로 사용하지만, 종종 공급망 공격을 함께 수행하기도 하며 안드로이드 스마트폰 이용자를 노린 모바일 공격도 함께 수행하고 있으므로 각별한 주의가 필요하며 특히 외교·안보·국방·통일 및 대북분야 종사자들은 경감심을 높여 항상 대비하는 자세와 노력이 요구되며 민관의 긴밀한 대응이 필요합니다.

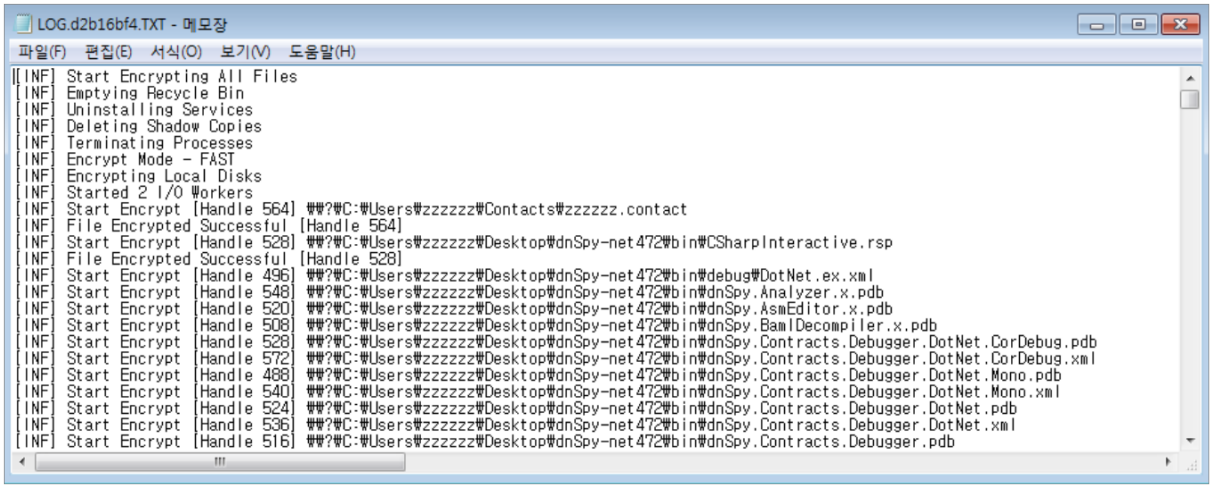
현재 이스트시큐리티 알약(ALYac)에서는 해당 악성코드 샘플을 'Trojan.Downloader.DOC.Gen, Trojan.Downloader.Script.gen, Trojan.Agent.111616K'로 탐지 중이며 관련된 IoC 는 쓰렛 인사이드(Threat Inside)에서 확인하실 수 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.DarkSide] 악성코드 분석 보고서

'콜로니얼 파이프라인'이 지난 7 일 동유럽 해킹 집단 '다크사이드'의 랜섬웨어 공격을 받아 버지니아, 사우스캐롤라이나 등 미국에서 주유 난이 시작되었다.

해당 집단은 지난달에도 이탈리아 최대 협동조합 신용 은행을 공격하여 시스템을 마비 시켰다.



[그림] 악성 행위 로깅 파일

DarkSide 랜섬웨어는 사용자 PC 의 데이터를 암호화하여 금전을 요구하는 악성코드이다. 서비스형 랜섬웨어(RaaS)로 사용자 PC 에 악성 행위 로그를 남기는 것이 특징이다.

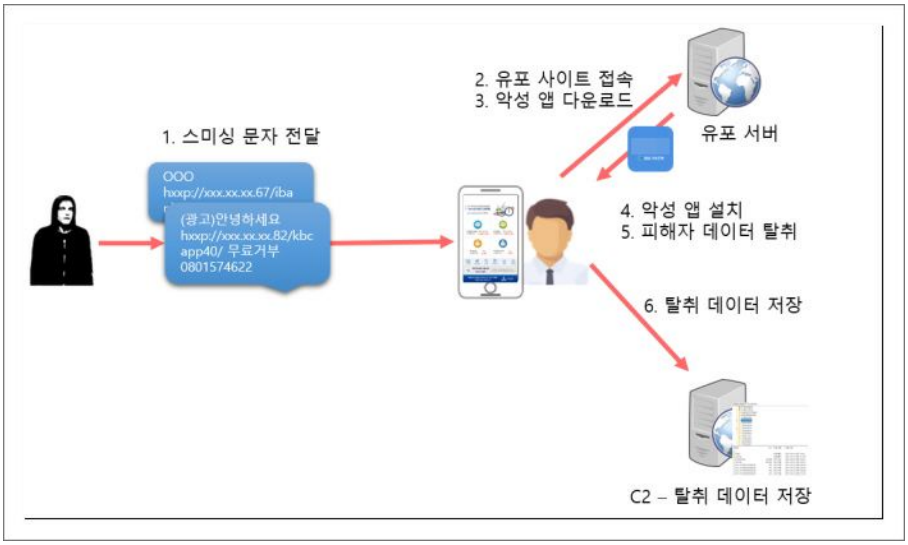
또한 로컬 드라이브와 네트워크 드라이브로 연결된 모든 파일을 암호화 대상에 포함하고 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

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 해당 악성코드를 'Trojan.Ransom.DarkSide' 탐지 명으로 진단하고 있으며, 관련 상세분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.KRBanker] 악성코드 분석 보고서

은행을 사칭하는 스미싱 공격의 특징은 링크로 접속 시 은행의 대출 관련 내용으로 꾸며진 가짜 웹페이지를 노출시킨다는 점이다. 때마침 피해자가 대출에 관심이 있다면 악성 앱을 다운로드해 설치하게 되며 공격자는 설치된 악성 앱을 통해 피해자의 개인 정보를 탈취하여 2 차 공격인 보이스피싱을 수행하게 된다.



[그림] 공격 흐름도

Trojan.Andorid.KRBanker 공격은 2 차 공격을 통한 금전 갈취가 주요 목적이다. 스미싱 공격의 표적이 되어 금전 갈취를 당하게 된다면 피해자는 경제적으로 심각한 타격을 입을 수도 있을 것이다. 따라서 스미싱 공격을 예방하기 위한 노력이 필요하다.

이런 스미싱 공격들의 피해 예방은 보기보다 간단하다. 수신 문자의 내용이 어색하거나 맞춤법 등에 실수가 많다면 문자 내의 URL 링크를 클릭하지 않거나 다운로드한 악성 앱을 설치하지 않으면 된다. 그리고 알약 M 과 같이 신뢰할 수 있는 백신 앱을 설치하여 사용하는 것도 피해를 예방하는 데 도움이 된다.

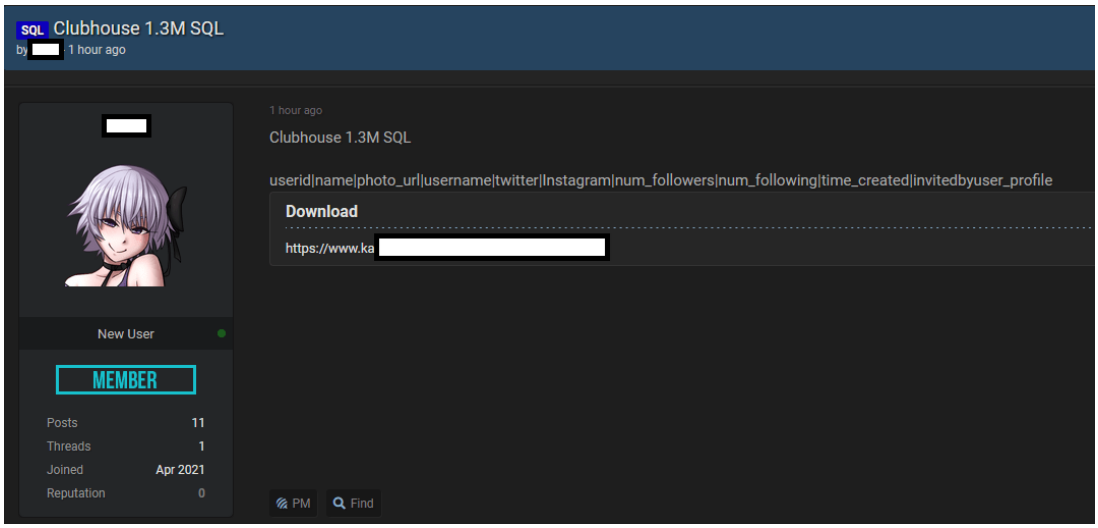
현재 알약 M 에서는 해당 앱을 ' Trojan.Android.KRBanker ' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

클럽하우스 사용자 130 만 명의 개인 데이터 온라인에 유출

Personal data of 1.3 million Clubhouse users leaked online

Cyber News 의 연구원들이 링크드인과 페이스북에 이어 클럽하우스 사용자 130 만 명의 개인 데이터가 온라인에 유출된 것을 발견했다. 연구원들은 한 해커 포럼에서 클럽하우스 사용자 130 만 명의 데이터가 포함된 SQL 데이터베이스를 무료로 제공한다는 광고를 발견했다.



[이미지 출처] https://cybernews.com/security/clubhouse-data-leak-1-3-million-user-records-leaked-for-free-online/

유출된 데이터에는 클럽하우스 사용자의 ID, 이름, 사용자명, 트위터 계정, 인스타그램 계정, 팔로워 수, 팔로잉 수, 계정 생성일, 해당 사용자가 초대한 사용자 이름 등이 포함되어 있었다. 금융 관련 데이터는 이 유출 사고에 포함되지 않았다. 전문가들은 해당 내용을 클럽하우스 측에 제보했지만, 클럽하우스는 아직까지 노출된 데이터의 진위 여부를 확인하지 않은 상태이다. 공격자는 유출된 데이터를 악용하여 피싱/스피어 피싱, 신원 도용, 사기 등 악성 공격을 수행할 수 있다. 전문가들은 이에 대해 다음과 같이 언급했다. “유출된 SQL 데이터베이스는 클럽하우스의 프로필 정보만 포함하고 있었다. 공격자가 공개한 아카이브에서 신용카드 정보, 법률 문서 등 민감 데이터는 찾아볼 수 없었다. 하지만 숙련된 사이버 범죄자들은 사용자의 다른 SNS 프로필과 연결된 프로필 이름만으로도 실제 피해를 입힐 수 있을 만큼 충분할 것이다."

지난 2 월, 한 공격자는 클럽하우스의 채팅 기능이 안전하지 않다는 것을 발견했다. 그는 여러 방의 오디오 피드를 그의 자체 웹사이트로 이동시킬 수 있었다. 클럽하우스는 2020 년 3 월에 출시된 초대 전용 SNS 앱으로, 사용자가 다양한 주제에 대해 토론하는 방이나 오디오 대화에 참여할 수 있도록 한다. 이 앱의 인기는 갈수록 커져 분석가들은 회사의 가치를 수십 억 달러로 평가했다. 클럽하우스 사용자들은 다음의 권장사항을 따를 것을 추천한다.

- 낯선 사람의 의심스러운 클럽하우스 메시지 및 연결 요청에 주의하기
- 이중 인증 기능 활성화하기
- 각 웹 서비스에 대해 강력하고 고유한 암호 사용하기
- 정보를 요구하는 잠재적 피싱 메시지 주의하기

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 피해자들이 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://blog.alyac.co.kr/3694

https://cybernews.com/security/clubhouse-data-leak-1-3-million-user-records-leaked-for-free-online/

Xcode 프로젝트를 통해 확산되는 XCSSET, M1 기반 Mac 기기 노려

Malware That Spreads Via Xcode Projects Now Targeting Apple's M1-based Macs

Xcode 개발자들을 노리는 한 Mac 악성코드 캠페인이 애플의 새로운 M1 칩을 지원하고, 가상화폐 앱으로부터 기밀 정보를 훔치는 기능을 추가하도록 업그레이드되었다. XCSSET 은 빌드 시 페이로드를 실행하도록 변조된 Xcode IDE 프로젝트를 통해 배포되었으며, 지난 2020 년 8 월 주목을 받았다.

이 악성코드는 합법적인 Mac 애플리케이션을 모방하기 위해 로컬 Xcode 프로젝트를 감염시키고 해킹된 프로젝트가 빌드될 때 메인 페이로드를 주입하는 역할을 하는 페이로드 모듈을 리패키징한다. XCSSET 모듈은 크리덴셜을 훔치고, 스크린샷을 캡처하고, 웹사이트에 자바스크립트를 주입하고, 다른 앱의 사용자 데이터를 약탈하고, 랜섬머니를 갈취하기 위해 파일을 암호화하는 기능을 포함하고 있다. 2021 년 3 월, 카스퍼스키 연구원들은 새로운 애플 M1 칩용으로 컴파일된 XCSSET 샘플을 발견하여 해당 악성코드 캠페인의 공격자가 캠페인을 진행 중임에도 적극적으로 실행파일을 조정하여 애플 실리콘을 탑재한 Mac 에서도 실행되도록 포팅하고 있음을 알 수 있었다.

```
if userName is equal to "apple_mac" then
        boot("chrome_remote", true)
        boot("firefox_remote", true)
        boot("opera_remote", true)
        boot("yandex_remote", true)
        boot("brave_remote", true)
        boot("edge_remote", true)
        boot("360_remote", true)
        boot("chromium_remote", true)
        return
end if
```

[이미지 출처] https://thehackernews.com/2021/04/malware-spreads-via-xcode-projects-now.html

Trend Micro 에서 실시한 가장 최근 연구에 따르면 XCSSET 은 UXSS(Universal Cross-site Scripting) 공격을 통해 웹사이트에 JavaScript 백도어를 심기 위해 사파리 브라우저의 개발 버전을 계속해서 악용하고 있는 것으로 나타났다. Trend Micro 는 지난 금요일 발행된 보고서에서 다음과 같이 밝혔다. "이는 C2 서버에 사파리 업데이트 패키지를 호스팅한 후 사용자의 OS 버전에 따른 패키지를 다운로드 및 설치한다. 새롭게 공개된 Big Sur 를 도입하기 위해 'Safari 14'용 패키지가 추가되었다."

이 악성코드는 사파리에서 데이터를 추출하기 위해 트로이목마화 하는 것 이외에도 UXSS 공격을 실행하기 위해 Google Chrome, Brave, Microsoft Edge, Mozilla Firefox, Opera, Qihoo 360 Browser, Yandex Browser 등 기타 브라우저의 원격 디버깅 모드를 악용하는 것으로도 알려져 있다. 게다가 이 악성코드는 Huobi, Binance, NNCall.net, Envato, 163.com 을 포함한 가상화폐 거래 플랫폼 등 웹사이트 다수에서 계정 정보를 훔치려 시도하기도 한다. 이는 사용자의 가상화폐 지갑 주소를 공격자의 주소로 바꿔치기하는 기능 또한 포함하고 있다. 조작된 Xcode 프로젝트를 통한 XCSSET 의 배포 모드는 심각한 위협이 된다. 영향을 받은 개발자가 자신의 작업을 무의식적으로 GitHub 에 공개할 경우, 해킹된 Xcode 프로젝트의 형태로 사용자들에게 악성코드를 배포할 수 있기 때문이다.

[출처]

https://blog.alyac.co.kr/3714

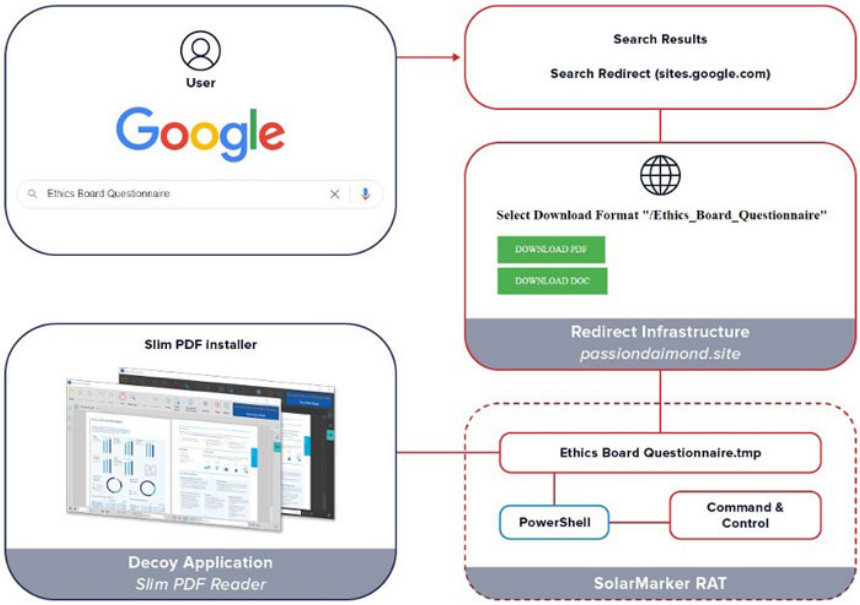
https://thehackernews.com/2021/04/malware-spreads-via-xcode-projects-now.html〉

악성 PDF 파일을 배포하는 웹 페이지 10 만 곳 이상 생성돼

YIKES! Hackers flood the web with 100,000 pages offering malicious PDFs

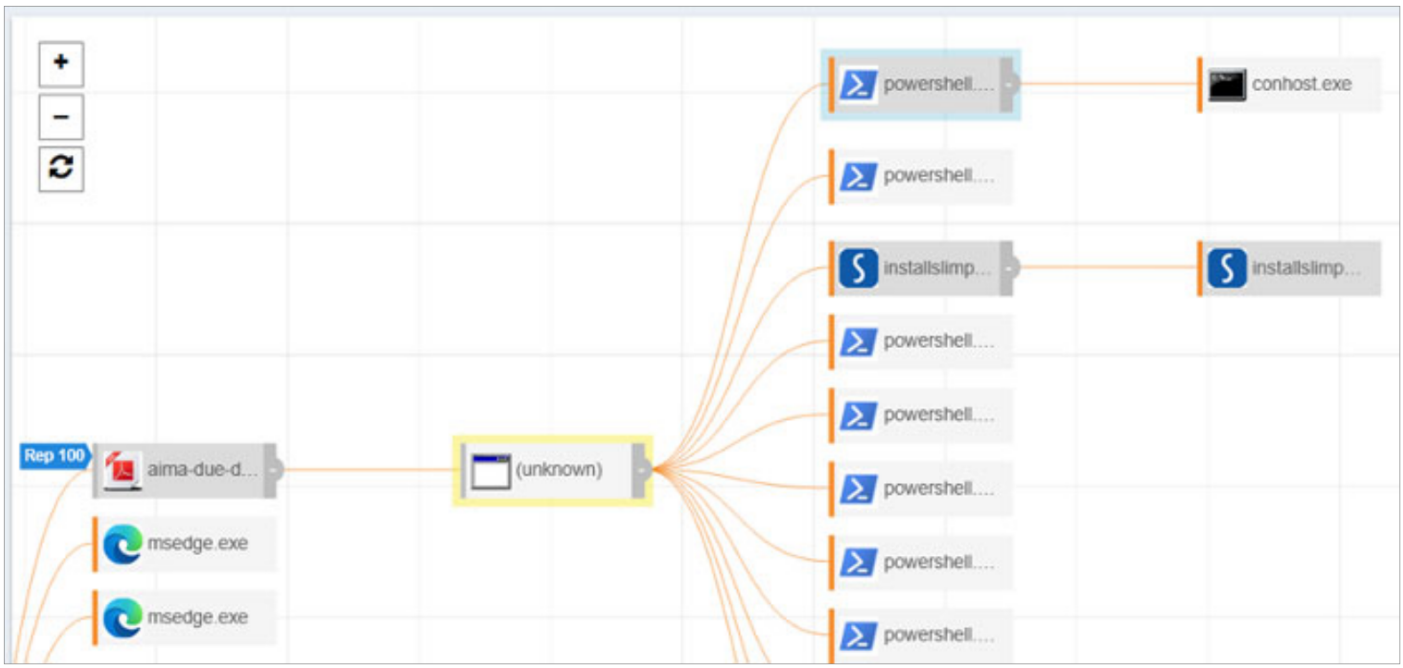
사이버 범죄자들이 정식 구글 사이트로 보이지만 다양한 공격을 수행하는 원격 액세스 트로이목마(RAT)를 설치하는 페이지로 비즈니스 전문가를 유인하기 위해 검색 엔진을 오염시키고 있는 것으로 나타났다.

이 공격은 인보이스, 템플릿, 설문지, 영수증 등 기업용 문서 양식에 대한 검색 결과를 악용한다. 악성 문서 템플릿을 다운로드하는 사용자는 자신도 모르는 사이 악성코드를 호스팅하는 악성 웹사이트로 이동된다. eSentire 의 연구원들은 이에 대해 다음과 같이 언급했다. "RAT 이 피해자의 컴퓨터에 설치되고 활성화되면, 공격자들은 감염된 시스템으로 명령을 전송하고 랜섬웨어, 크리덴셜 스틸러, 뱅킹 트로이목마, 피해자의 네트워크에 침투할 발판으로 삼을 RAT 등 추가 악성코드를 업로드할 수 있게 된다."



[이미지 출처] https://www.esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire

해당 보안 회사는 템플릿, 인보이스, 영수증, 설문지, 이력서 등 인기있는 비즈니스 용어나 키워드를 포함한 고유 웹 페이지 10 만 개 이상을 발견했다고 밝혔다. 따라서 이 페이지는 검색 결과 상단에 위치하게 되어 공격의 성공률을 높이는 것이 가능하다. 일단 피해자가 공격자가 제어하는 웹사이트에 도착해 검색을 시도한 문서를 다운로드하면, 이는 더욱 정교한 공격을 실행할 수 있는 진입점이 되어 결국 .NET 기반 RAT 인 SolarMarker(Yellow Cockatoo, Jupyter, Polazert 로도 알려짐)를 설치하게 된다. 재무 관리 회사의 한 직원이 참여한 한 사례에 따르면 이 악성코드 실행파일은 PDF 문서로 위장하고 있었으며, 실행될 경우 RAT 과 함께 미끼로 Slim PDF 의 정식 버전을 배포했다.



[이미지 출처] https://www.esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire

eSentire 은 이 캠페인의 또 다른 문제로 “SolarMarker 그룹이 그들의 악성 웹 페이지에 재무 문서와 관련된 키워드를 많이 사용한 것이다. 재무 관련 사이버 범죄 그룹은 회사의 재무 부서에서 일하는 직원이나 금융 기관 직원을 고가치 타깃으로 간주할 것이다. 안타깝게도 일단 RAT 이 설치될 경우 실행 가능한 잠재적 사기 행위는 무궁무진하다.”고 밝혔다.

[출처]

https://blog.alyac.co.kr/3703

https://www.esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire

(주)이스트시큐리티

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