이스트시큐리티

보안 동향 보고서

No.141 2021.06

No.141 2021.06

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 5 월도 지난달과 마찬가지로 국내외 다양한 조직들을 타깃으로 한 지속적인 APT 공격이 다수 포착되었습니다.

5 월 초, 국내 중소기업 임직원 메일 계정을 사칭한 피싱 메일이 발견됐습니다. 발견된 피싱 메일은 경기 지역에 위치한 한 기계 제조 업체의 임직원 이름과 이메일 계정을 사칭했으며, 해당 업체명이 포함된 제목을 사용했습니다. 또한 발신자로 악용된 직원 이름은 해당 기업명을 검색했을 때 우선순위가 높게 나타나는 LinkedIn 프로필을 통해 쉽게 확인할 수 있었습니다. 피싱 메일에 포함된 첨부파일은 인포스틸러 악성코드인 Lokibot 감염으로 이어지며, 감염된 PC 에 설치된 다양한 프로그램에서 자격 증명 정보가 탈취됩니다.

이번 달에는 정부 기관 및 기업 관계자를 넘어서 국내 일반 사용자들을 타깃으로 한 공격도 포착됐습니다. 해당 공격에 사용된 피싱 메일은 국내 유명 대학교의 교직원 장학금 신청 관련 내용으로 위장했으며, 본문은 한글과 영어 버전이 모두 작성되어 있어, 수신자의 국적과 관계없이 첨부파일을 열어보도록 유도했습니다. 또한 메일에 사용된 발신 주소 도메인도 실제로 존재하는 스페인, 캐나다 등의 해외 기업으로 신뢰성을 높였습니다. 해당 공격을 통해 감염되는 악성코드도 사용자 PC 내 다양한 정보를 수집하는 악성코드입니다. 따라서 관련 악성코드 감염을 예방하기 위해 출처가 불분명한 이메일의 첨부파일 혹은 URL 클릭을 삼가야 하며, 백신 소프트웨어를 최신 버전으로 설치하고 정기적인 검사를 습관화해야 합니다. 국내외 다양한 조직을 타깃으로 삼은 피싱 공격의 상세한 분석 내용 및 IoC 정보는 이스트시큐리티 알약 블로그 및 Threat Inside 에서 확인할 수 있습니다.

최근 랜섬웨어 공격자들이 고도화된 공격 기법과 랜섬머니 갈취 작전으로 활발한 활동을 펼치고 있습니다. 미국에서는 DarkSide 랜섬웨어 운영 조직이 ‘Colonial Pipeline’을 공격해 시스템이 중단되고 주유난이 발생하기도 했습니다. 국내에서도 배달대행 플랫폼 ‘슈퍼히어로’가 랜섬웨어 공격을 받아 35 시간 만에 서버를 복구하기도 했습니다. 당시 슈퍼히어로 측은 해커가 요구한 비트코인을 송금했으나, 해커가 잠적하면서 서버 복구가 지연됐습니다. 이처럼 랜섬웨어 공격을 받을 경우 랜섬머니를 지불하더라도 정상적으로 시스템을 복구하기 어려울 가능성이 큽니다.

따라서 기업 관계자를 비롯한 모든 사용자는 항상 컴퓨터 및 인터넷 사용 습관에 주의해야 하며 주기적인 시스템 백업과 함께 사이버 보안에 관심을 갖는 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 5 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Hosts.media.opencandy.com 이 1 위를 차지했으며, 지난달 6 위를 차지했던 Misc.Riskware.BitCoinMiner 가 탐지율 급등으로 2 위를 차지했다. JS:Trojan.Cryxos.5628 을 비롯한 3 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 눈에 띄는 부분으로는 Misc.Riskware.Segurazo 가 지난달 순위에서 10 계단 상승하여 3 위를 차지했으며, 그 외에는 15 위 이내에서 큰 변동 없이 대체적으로 지난달과 유사한 순위 양상을 보였다.

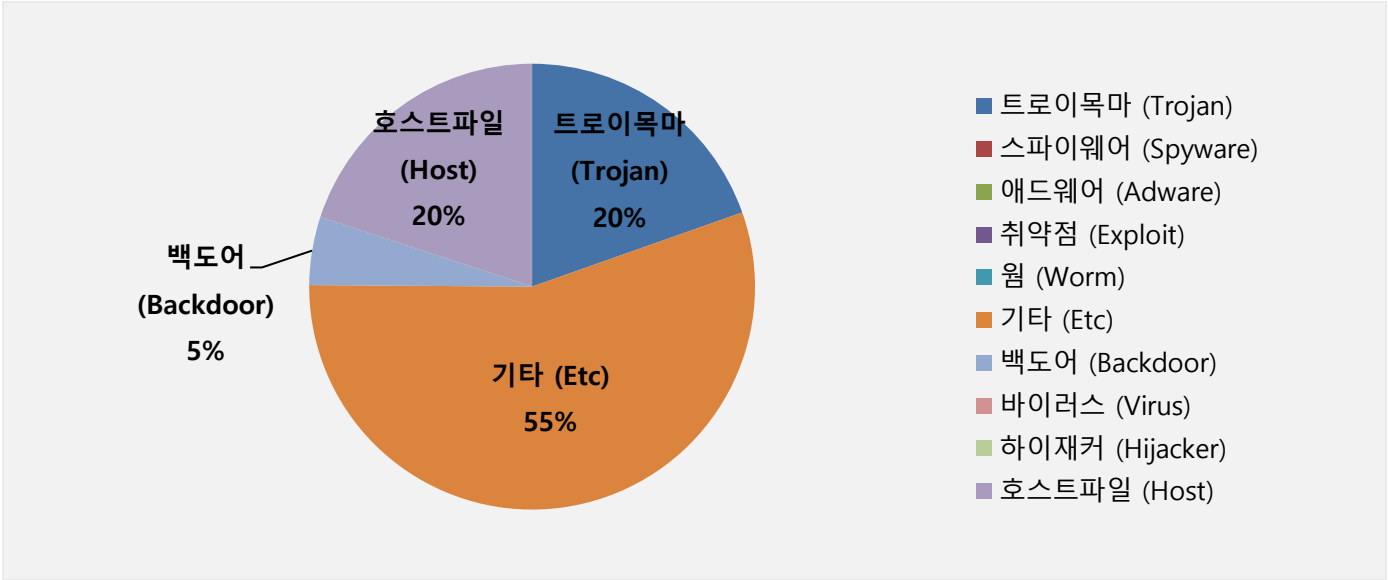
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	643,407
2	↑ 4	Misc.Riskware.BitCoinMiner	ETC	543,895
3	↑ 10	Misc.Riskware.Segurazo	ETC	371,700
4	↓ 2	Misc.HackTool.AutoKMS	ETC	338,551
5	↓ 2	Trojan.ShadowBrokers.A	Trojan	177,753
6	↓ 2	Trojan.Agent.Injector.Gen	ETC	170,930
7	-	Backdoor.Generic.792814	Backdoor	159,620
8	↓ 3	Misc.HackTool.KMSActivator	ETC	154,988
9	↑ 3	Misc.Riskware.TunMirror	ETC	109,500
10	↓ 2	Trojan.GenericKD.46161563	Trojan	108,103
11	New	JS:Trojan.Cryxos.5628	Trojan	107,526
12	↓ 1	Misc.Keygen	ETC	101,219
13	New	Gen:Trojan.Dropper.RQU.Gv1@aOQJORpO	Trojan	86,746
14	New	Trojan.GenericKD.46266871	Trojan	76,369
15	↓ 1	Trojan.Agent.Gen	Trojan	75,816

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 05 월 01 일 ~ 2021 년 05 월 31 일

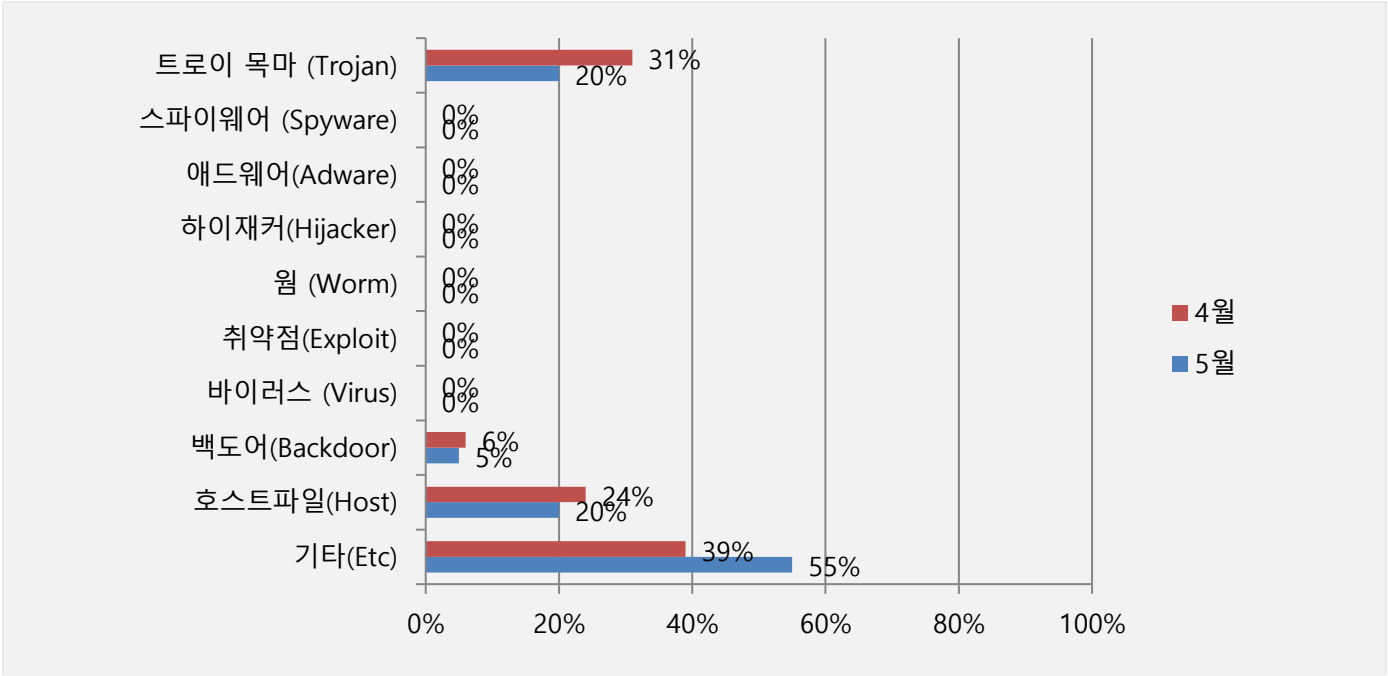
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 55%를 차지했으며 트로이목마(Trojan) 유형과 호스트파일(Host) 유형이 동일하게 20%로 그 뒤를 이었다. 지난달 6%를 차지했던 백도어(Backdoor) 악성코드 유형은 1% 감소하여 5% 를 기록했다. 2021 년 4 월과 비교하여 전체 감염 건수는 약 11.83% 증가하였다. .



카테고리별 악성코드 비율 전월 비교

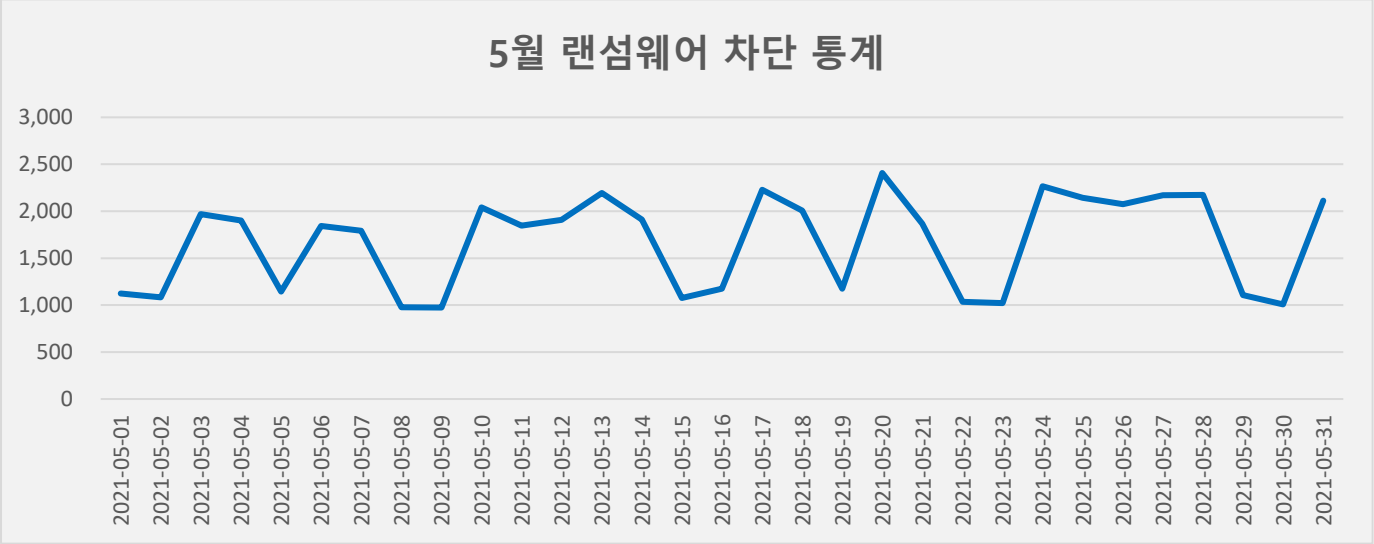
5 월에는 지난 4 월과 비교하여 트로이목마(Trojan) 유형이 11% 감소하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 4% 감소했다. 4 월에 6%를 차지했던 백도어(Backdoor) 유형이 소폭 감소하여 5%를 기록했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

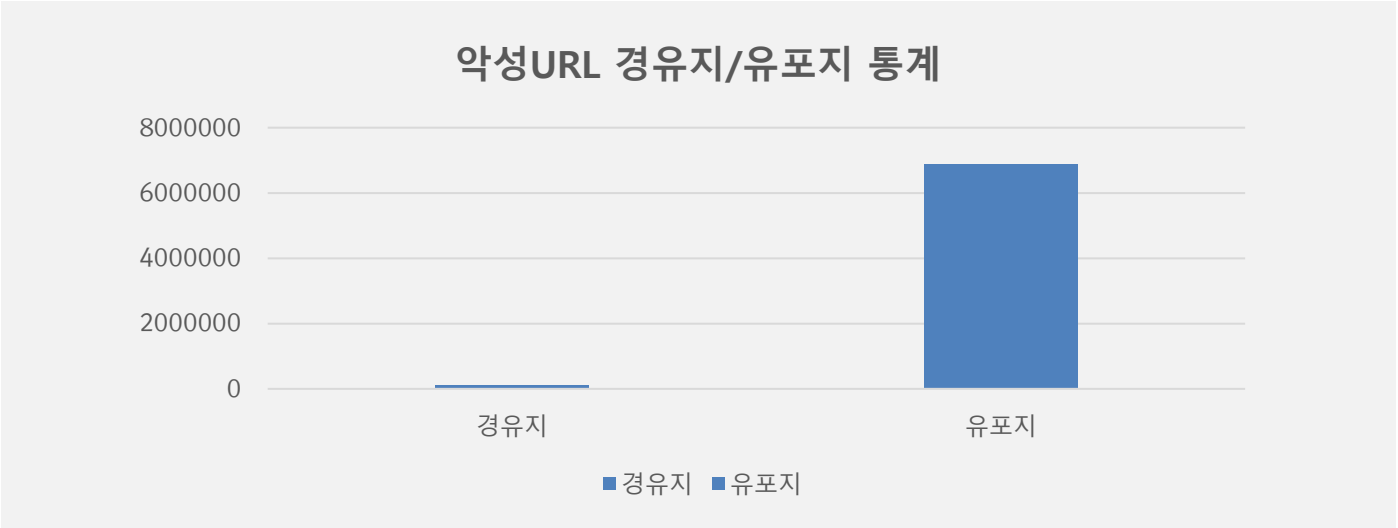
5 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 5 월 1 일부터 5 월 31 일까지 총 51,742 건의 랜섬웨어 공격 시도가 차단되었다. 4 월의 랜섬웨어 공격 건수인 52,742 건에 비해 약 1.9% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 5 월 한 달간 총 6,976,796 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 4 월 한 달간 확인되었던 6,585,240 건의 악성코드 경유지/유포지 URL 수에 비해 약 5.95% 가량 증가한 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

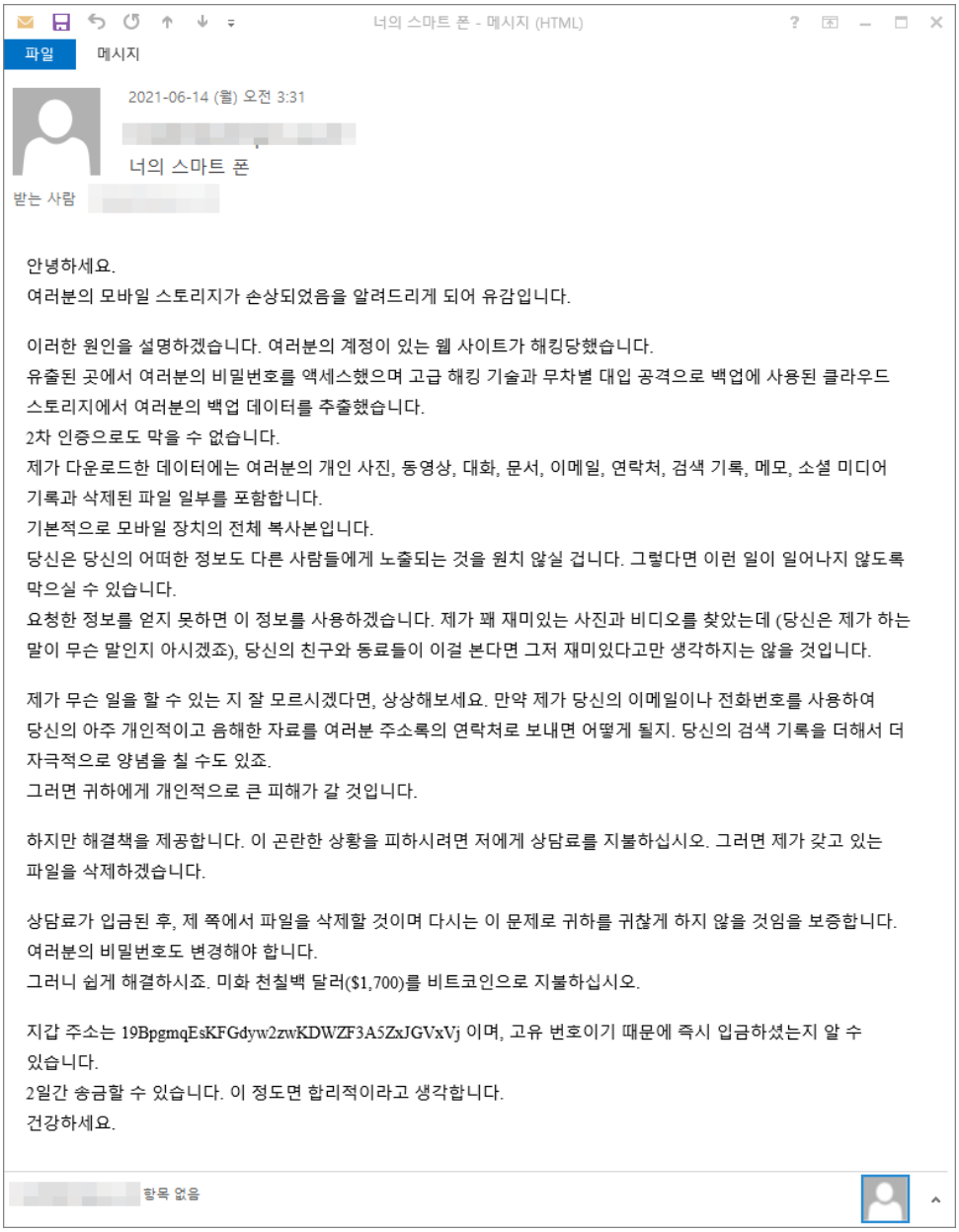
1. ‘스마트폰 클라우드 스토리지 해킹’으로 협박하는 혹스(Hoax)메일 주의

2. 국내 유명은행 보안메일을 사칭한 RemcosRAT 악성 이메일 주의

1. 스마트폰 클라우드 스토리지 해킹'으로 협박하는 혹스(Hoax)메일 주의

6월 14일 오전 3시부터 국/내외 불특정 다수의 사용자에게 협박성 Hoax 이메일이 유포되고 있어 사용자들의 주의가 필요합니다.

이번에 발견된 메일은 "너의 스마트폰" 이라는 제목으로 전파되고 있으며, 사용자의 모바일 복사본이 업로드되어있는 클라우드 스토리지 사이트가 해킹되어 모든 정보를 가지고 있으니 음란한 자료를 지인에게 보낼 수 있으니 상담료를 보내라는 협박 내용들이 기재되어 있습니다.



[그림 1] 유포되고 있는 Hoax 메일 화면

02 전문가 기고

현재 유포 중인 혹스(Hoax) 메일 본문의 전체 내용은 아래와 같습니다.

안녕하세요.
여러분의 모바일 스토리지가 손상되었음을 알려드리게 되어 유감입니다.

이러한 원인을 설명하겠습니다. 여러분의 계정이 있는 웹 사이트가 해킹당했습니다.
유출된 곳에서 여러분의 비밀번호를 액세스했으며 고급 해킹 기술과 무차별 대입 공격으로 백업에 사용된 클라우드 스토리지에서 여러분의 백업 데이터를 추출했습니다.
2 차 인증으로도 막을 수 없습니다.
제가 다운로드한 데이터에는 여러분의 개인 사진, 동영상, 대화, 문서, 이메일, 연락처, 검색 기록, 메모, 소셜 미디어 기록과 삭제된 파일 일부를 포함합니다.
기본적으로 모바일 장치의 전체 복사본입니다.
당신은 당신의 어떠한 정보도 다른 사람들에게 노출되는 것을 원치 않실 겁니다. 그렇다면 이런 일이 일어나지 않도록 막으실 수 있습니다.
요청한 정보를 얻지 못하면 이 정보를 사용하겠습니다. 제가 꽤 재미있는 사진과 비디오를 찾았는데 (당신은 제가 하는 말이 무슨 말인지 아시겠죠), 당신의 친구와 동료들이 이걸 본다면 그저 재미있다고만 생각하지는 않을 것입니다.

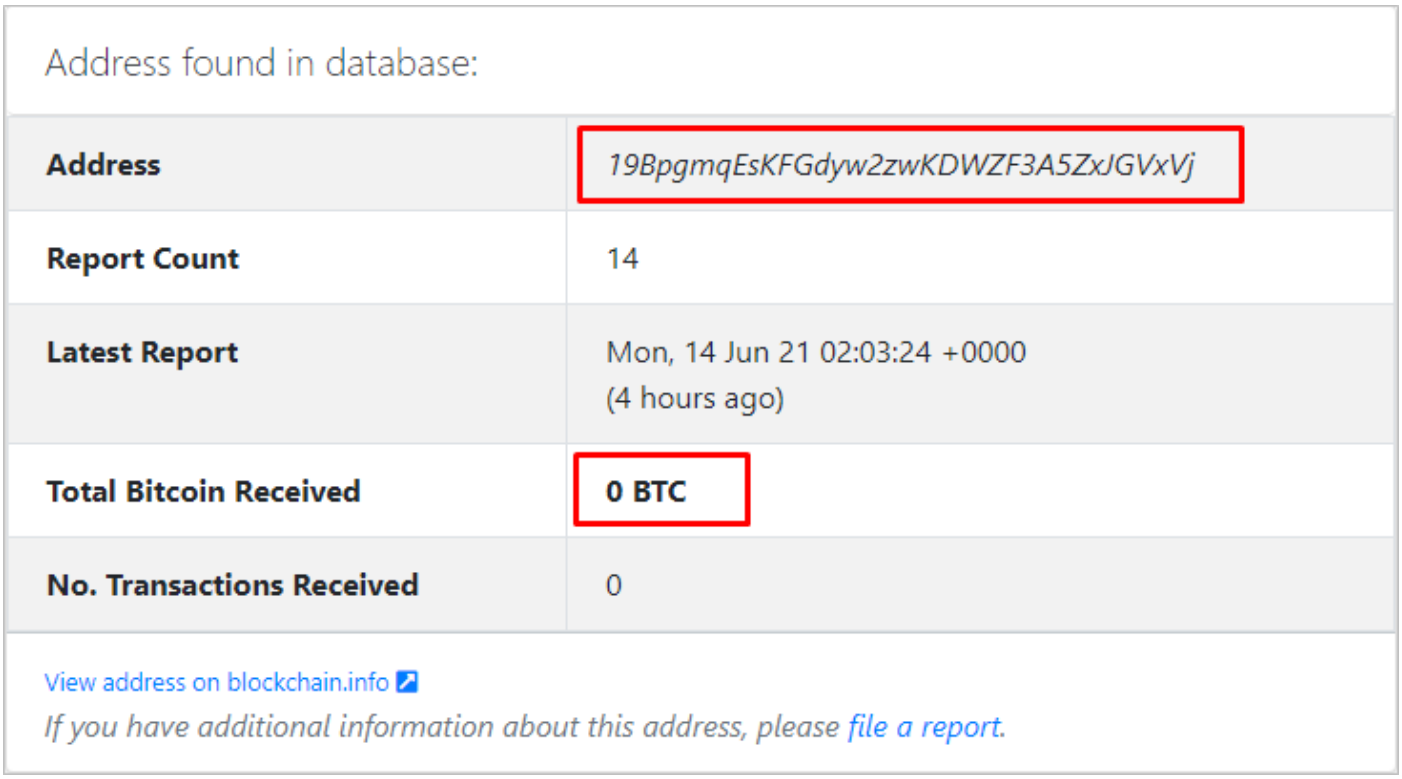
제가 무슨 일을 할 수 있는 지 잘 모르시겠다면, 상상해보세요. 만약 제가 당신의 이메일이나 전화번호를 사용하여 당신의 아주 개인적이고 음해한 자료를 여러분 주소록의 연락처로 보내면 어떻게 될지. 당신의 검색 기록을 더해서 더 자극적으로 양념을 칠 수도 있죠.
그러면 귀하에게 개인적으로 큰 피해가 갈 것입니다.

하지만 해결책을 제공합니다. 이 곤란한 상황을 피하시려면 저에게 상담료를 지불하십시오. 그러면 제가 갖고 있는 파일을 삭제하겠습니다.

상담료가 입금된 후, 제 쪽에서 파일을 삭제할 것이며 다시는 이 문제로 귀하를 귀찮게 하지 않을 것임을 보증합니다. 여러분의 비밀번호도 변경해야 합니다.
그러니 쉽게 해결하시죠. 미화 천칠백 달러($1,700)를 비트코인으로 지불하십시오.

지갑 주소는 19BpgmqEsKFGdyw2zwKDWZF3A5ZxJGVxVj 이며, 고유 번호이기 때문에 즉시 입금하셨는지 알 수 있습니다.
2 일간 송금할 수 있습니다. 이 정도면 합리적이라고 생각합니다.
건강하세요.

이번 메일에서 사용된 제작자의 비트코인 주소는 수익을 얻지 못한 상태입니다.



Address found in database:

Address	*19BpgmqEsKFGdyw2zwKDWZF3A5ZxJGVxVj*
Report Count	14
Latest Report	Mon, 14 Jun 21 02:03:24 +0000 (4 hours ago)
Total Bitcoin Received	**0 BTC**
No. Transactions Received	0

View address on blockchain.info

If you have additional information about this address, please file a report.

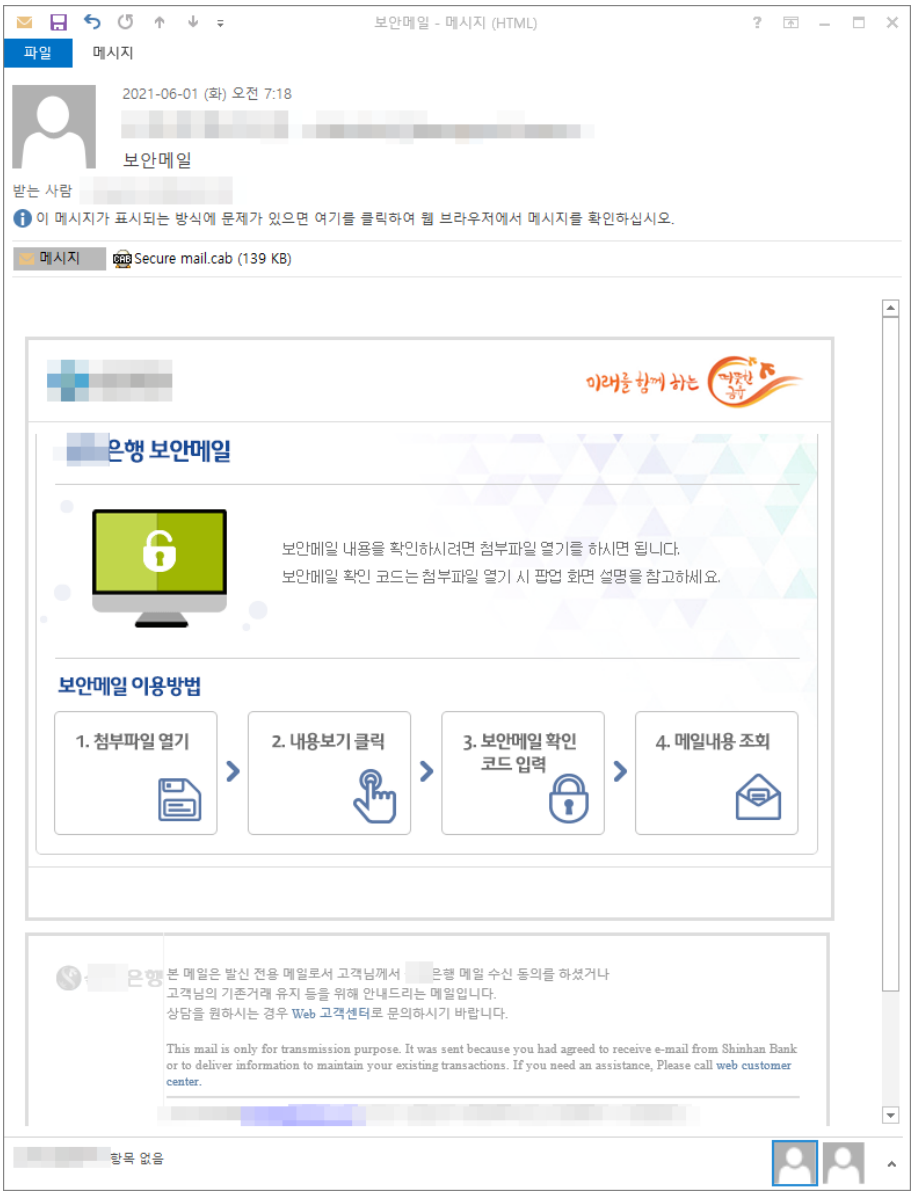
[그림 2] 혹스(Hoax) 메일 발신자의 비트코인 수익 화면

기존까지의 Hoax 메일은 대부분 사용자의 데스크톱이나 노트북을 해킹하여 사생활 녹화 영상을 빌미로 협박하는 경우가 많았지만, 이번에 발견된 Hoax 메일은 최근 트렌드에 맞추어 많은 사람들이 사용하는 스마트폰으로 협박하기 때문에 이전 메일보다 쉽게 속을 수 있습니다. 이러한 메일처럼 금전을 요구하는 메일은 바로 삭제하는 것을 권장합니다.

2. 국내 유명 은행 보안메일을 사칭한 RemcosRAT 악성 이메일 주의

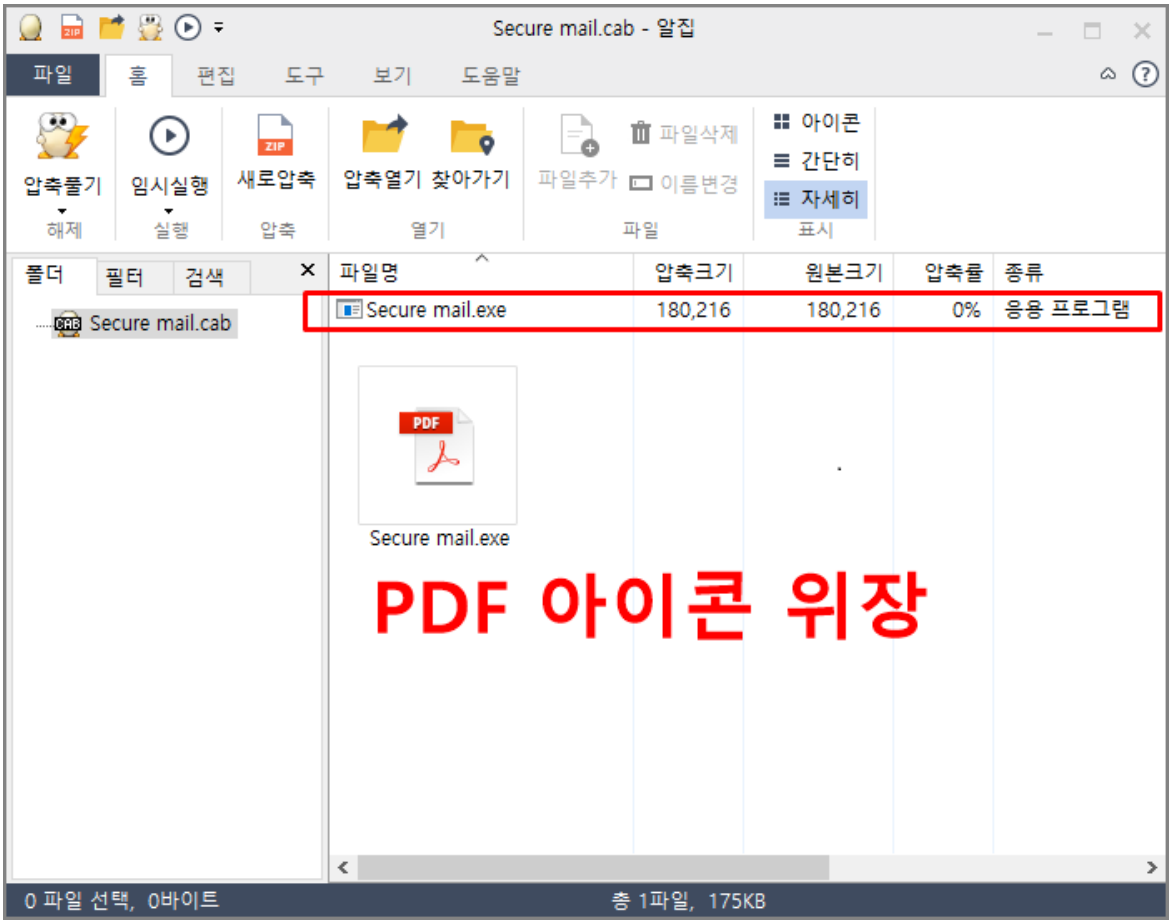
최근 국내 유명 은행 보안메일을 사칭한 악성 이메일이 발견되어 사용자들의 주의가 필요합니다.

이번에 발견된 메일은 "보안메일"이라는 제목을 사용하며, 실제 해당 은행에서 보내는 보안메일과 유사하게 제작되었습니다.



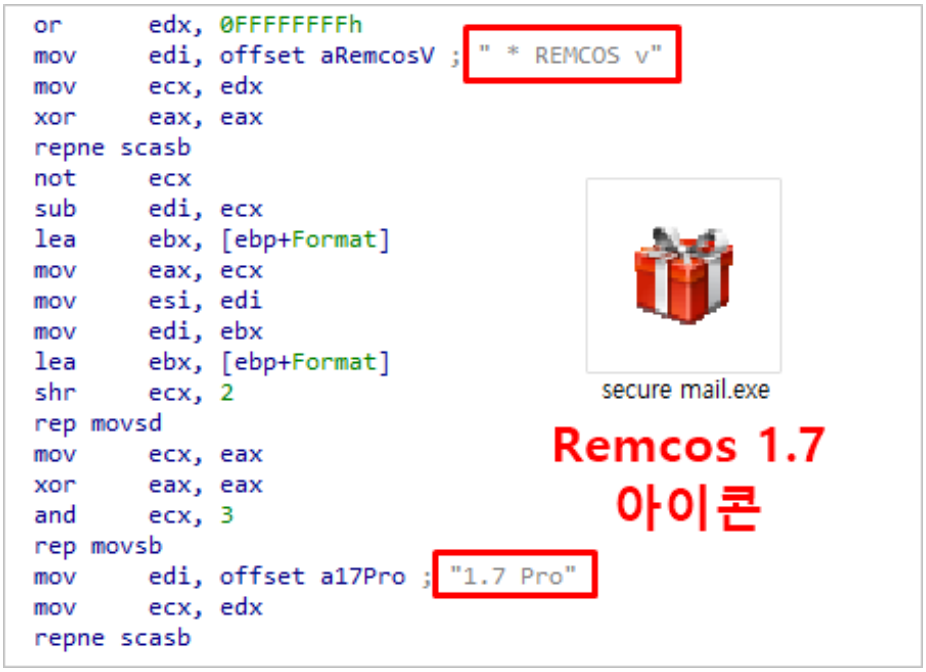
[그림 1] 은행 보안메일 사칭 악성 이메일

보안메일 프로그램처럼 보이는 첨부 파일은 “PDF 문서 아이콘”으로 위장하여 사용자가 다운로드하여 실행 시 악성 행위를 시작합니다.



[그림 2] 첨부파일 내부 화면

악성파일은 Remcos Rat 1.7 Pro 버전으로 확인되었으며 진단을 우회하기 위해 .NET을 이용하였으나, 내부 악성 모듈을 추출하면 버전 정보가 하드코딩되어 있습니다.



[그림 3] 하드코딩 된 Remcos Rat 버전 정보

02 전문가 기고

Remcos 악성코드는 명령제어 악성코드로, C&C 통신 이후 공격자 명령에 따라 다음과 같은 기능을 수행합니다.

명령어	설명
filemgr, upload, rename, deletefile, downloadfromurltofile	파일관리 (업로드, 다운로드, 파일명변경, 파일삭제)
regopened, regcreatekey, regeditval, regdelkey, regdelval, regopen, initregedit	레지스트리 관리(값 및 키 추가, 편집, 이름 바꾸기, 삭제)
getproclist, prockill	프로세스 관리 (프로세스 리스트 및 종료)
keyinput	키로깅
consolecmd, execcom, cmdoutput, sendfiledata	셸 명령 실행 및 결과 업로드
scrcap	화면 스크린샷
OSpower	시스템 종료 및 재시작

이외에도 사용자 PC 에 동작 중인 브라우저(Internet Explorer, Chrome, Firefox)의 쿠키 데이터와 로그인 정보를 수집합니다.

```
000000010AD1   000000410AD1      0   [Chrome StoredLogins found, cleared!]
000000010AF9   000000410AF9      0   [Chrome StoredLogins not found]
000000010B1C   000000410B1C      0   UserProfile
000000010B28   000000410B28      0   \AppData\Local\Google\Chrome\User Data\Default\Login Data
000000010B65   000000410B65      0   [Chrome Cookies found, cleared!]
000000010B89   000000410B89      0   [Chrome Cookies not found]
000000010BA4   000000410BA4      0   \AppData\Local\Google\Chrome\User Data\Default\Cookies


000000010BDD   000000410BDD      0   [Firefox StoredLogins cleared!]
000000010C00   000000410C00      0   \key3.db
000000010C0C   000000410C0C      0   \logins.json
000000010C21   000000410C21      0   [Firefox StoredLogins not found]
000000010C44   000000410C44      0   \AppData\Roaming\Mozilla\Firefox\Profiles\
000000010C71   000000410C71      0   [Firefox cookies found, cleared!]
000000010C94   000000410C94      0   \cookies.sqlite
000000010CA5   000000410CA5      0   [Firefox Cookies not found]


000000010CC9   000000410CC9      0   [IE cookies cleared!]
000000010CE1   000000410CE1      0   [IE cookies not found]
000000010CF8   000000410CF8      0   Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
000000010D40   000000410D40      0   Cookies
```

[그림 4] 브라우저 정보 탈취 기능

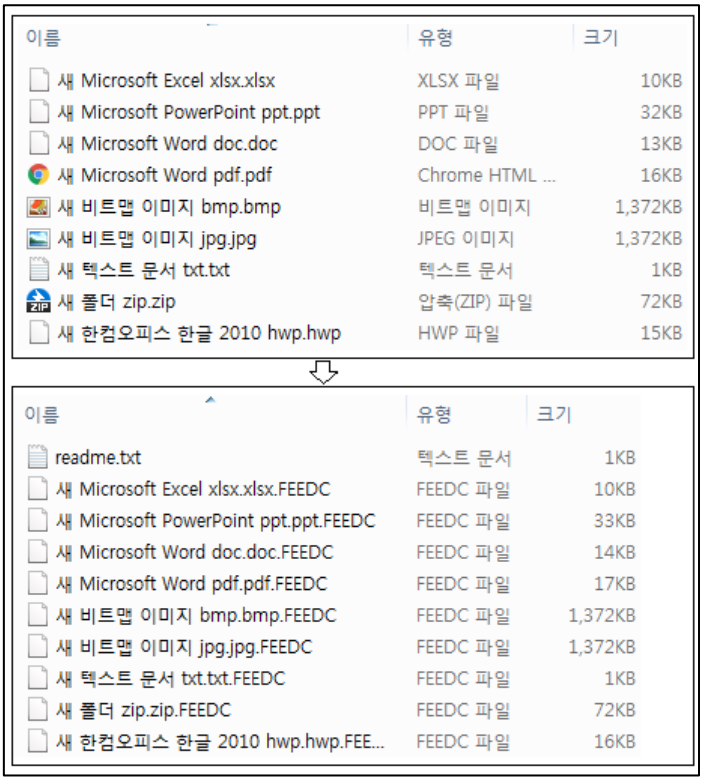
현재 알약에서는 해당 악성코드에 대해 Backdoor.Remcos.A 로 탐지 중에 있으며, 관련 IoC 는 Threat Inside 에서 확인하실 수 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.Conti] 악성코드 분석 보고서

Trojan.Ransom.Conti'(이하 'Conti') 랜섬웨어는 2019 년 12 월에 처음 배포된 것으로 확인됐다. 최근 400 개 이상의 조직이 Conti 랜섬웨어 공격의 표적이 되었으며, 16 건의 공격은 의료 기관 시스템에서 알려졌다.

Conti 랜섬웨어는 파일 암호화 기능을 수행하는 랜섬웨어이다. 랜섬노트에서 안내되는 다크넷에서 추가로 대화가 입력되면서 이용자에게 금전을 탈취하는 점이 특징이다.



[그림] 암호화 전/후

랜섬웨어의 특성 상, 기업체나 일반 이용자 입장에서 사용자 정보가 담긴 파일을 암호화할 수 있기 때문에 금전, 정보 유출 등의 피해가 발생될 수 있어 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 혹은 URL 클릭을 삼가야 하며, 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

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

[Trojan.Android.KRBanker] 악성코드 분석 보고서

최근 발견되는 악성 앱 중 피해자의 금전 탈취를 위해 정교하게 만들어진 앱을 살펴보도록 하겠다.

해당 앱은 예전부터 주기적으로 확인되었으며 현재까지 매주 1~2 개씩 발견되고 있다. 또한, 목적이 보이스 피싱 공격이므로 공격 흐름은 악성 앱을 해당 기기에 설치하는 것부터 시작된다. 이후 개인 정보 탈취를 비롯한 스마트폰의 통화 기능을 장악하여 피해자의 통화를 유도하고 변조하여 최종 목표인 금전 탈취를 달성하게 된다.

[그림] 앱 실행 화면

Trojan.Android.Banker 는 보이스 피싱 공격을 통해 피해자의 금전 갈취를 주요 목적으로 하고 있다. 각종 신뢰할 수 있는 기관이나 은행들을 사칭하여 피해자가 구별하기 더욱 힘들게 하고 있다. 따라서 이런 공격은 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 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

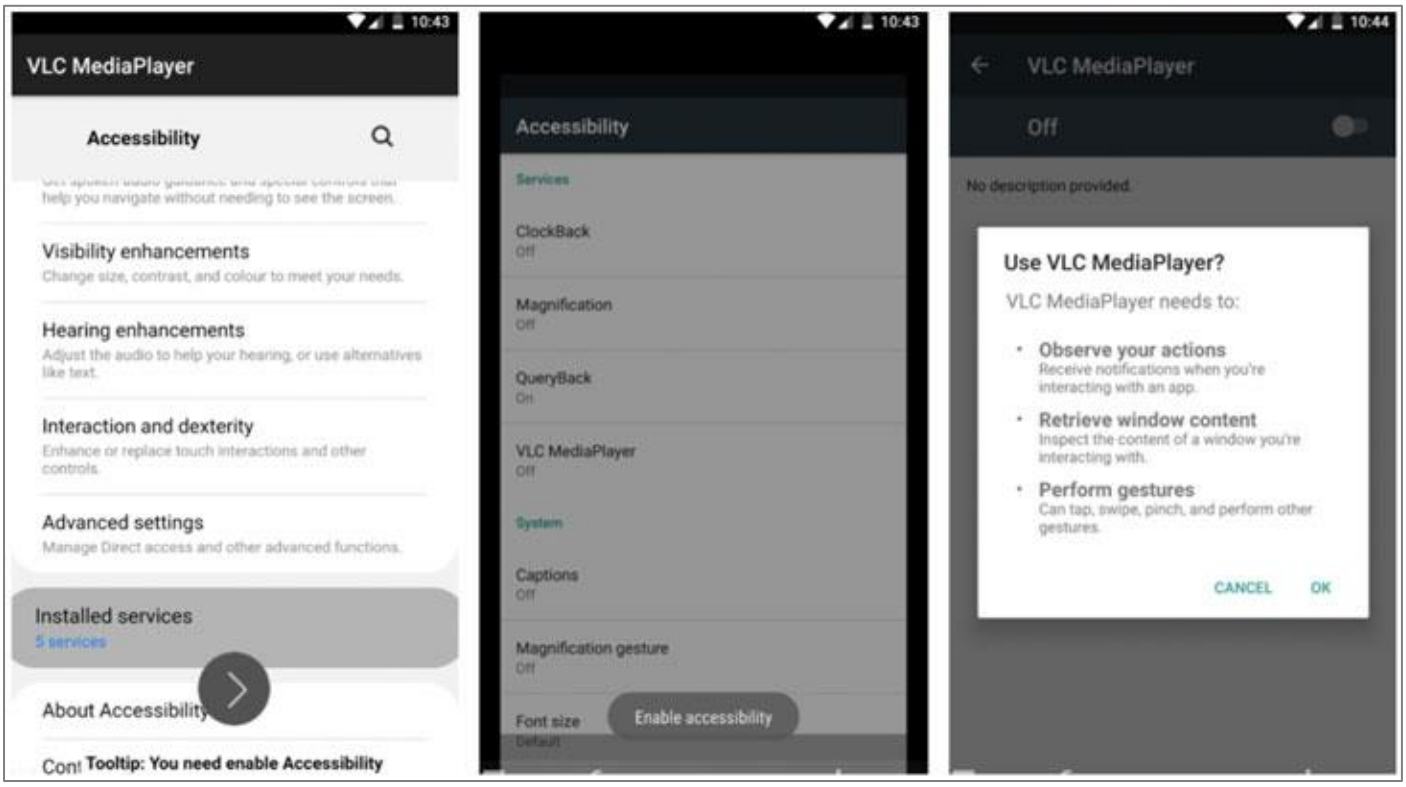
사용자의 크리덴셜을 훔치는 새로운 안드로이드 뱅킹 트로이목마 발견

Experts warn of a new Android banking trojan stealing users' credentials

스페인, 독일, 이탈리아, 벨기에, 네덜란드 내 은행을 통한 사기 행위를 저지르기 위해 사용자의 크리덴셜 및 SMS 메시지를 훔치는 새로운 안드로이드 트로이목마가 발견됐다. 'TeaBot' 또는 'Anatsa'라 명명된 이 악성코드는 아직까지 개발 초기 단계인 것으로 알려졌다. 금융 앱을 노리는 악성 공격은 2021 년 3 월 말 시작되었으며, 5 월 첫 주에 벨기에와 네덜란드 은행 관련 감염이 급격히 증가했다. TeaBot 활동의 첫 징후는 1 월경 나타났다.

이탈리아의 사이버 보안 및 온라인 사기 예방 회사인 Cleafy 는 이에 대해 다음과 같이 언급했다. “TeaBot 의 주요 목표는 미리 정의된 은행 목록에 대한 사기 공격을 실행하기 위해 피해자의 크리덴셜 및 SMS 메시지를 훔치는 것이다.

TeaBot 이 피해자 기기에 성공적으로 설치되면, 공격자들은 기기 화면을 실시간 스트리밍으로 볼 수 있으며, 접근성 서비스를 통해 기기와 상호작용이 가능하게 된다.” TeaTV, VLC Media Player, DHL, UPS 와 같은 미디어 및 택배 서비스로 위장한 악성 안드로이드 애플리케이션은 2 단계 페이로드를 로드하는 드롭퍼 역할 뿐 아니라 피해자가 접근성 서비스 권한을 부여하도록 강제한다.



[이미지 출처] https://www.cleafy.com/documents/teabot

TeaBot 은 공격 체인의 마지막 단계에서 해킹된 기기와 실시간으로 상호작용하여 키 입력을 기록하고, 스크린샷을 캡처하고, 크리덴셜 및 신용카드 정보를 훔치기 위해 뱅킹 앱의 로그인 화면 위에 악성 오버레이를 표시하는 것이 가능하다. TeaBot 의 또 다른 기능은 Google Play Protect 비활성화, SMS 메시지 가로채기, 구글 인증기 2FA 코드 접근 등이 있다. 수집된 정보는 매 10 분 마다 공격자가 제어하는 원격 서버로 전송된다.

데이터 탈취를 위해 안드로이드의 접근성 서비스를 악용하는 악성코드가 최근 몇 개월 동안 급증하고 있다. 올해 초부터 Oscorp, BRATA, FluBot 등 악성코드 패밀리 최소 3 개에서 이 기능을 악용하여 감염된 기기를 완전히 제어했다. TeaBot 은 Flubot 과 동일하게 정상적인 배송 앱으로 위장한 미끼를 사용하는데, 이는 탐지를 피하기 위한 시도일 가능성이 있다. 지난 달, 독일과 영국에서는 FluBot 감염이 급증해 사기성 SMS 메시지를 통해 사용자가 “비밀번호 및 기타 민감 데이터를 훔치는 스파이웨어”를 설치하도록 속이는 지속적인 공격에 대한 경고를 발행했다.

[출처]

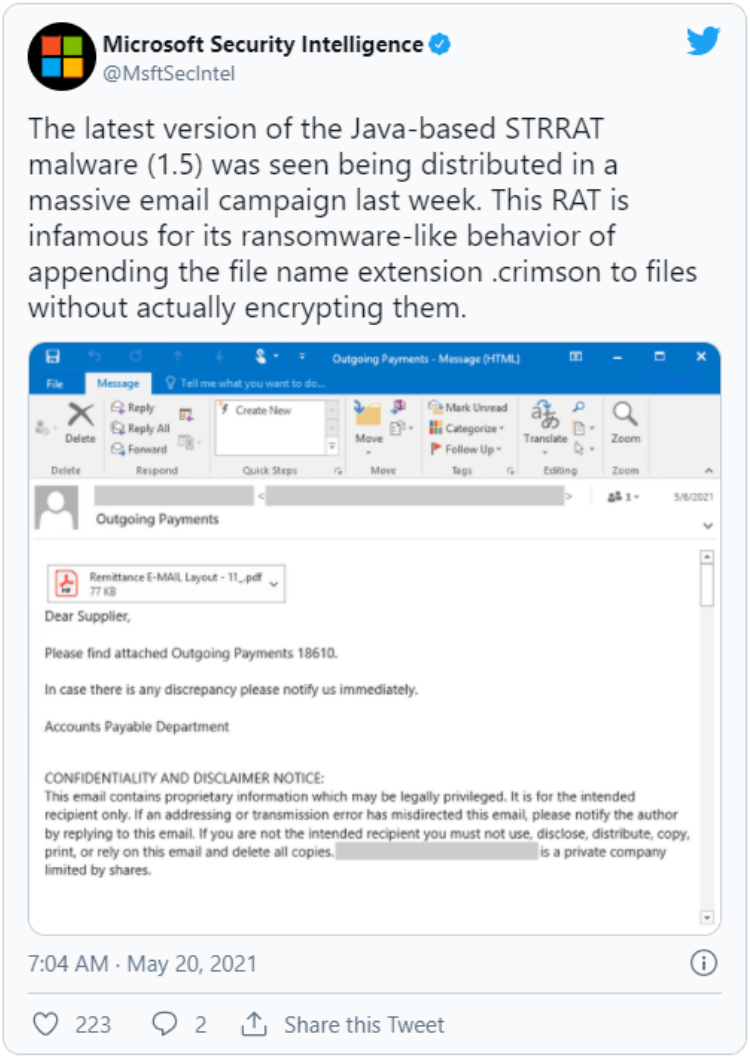
https://thehackernews.com/2021/05/experts-warn-of-new-android-banking.html

https://www.cleafy.com/documents/teabot

STRRAT RAT, 랜섬웨어로 위장하여 확산돼

STRRAT RAT spreads masquerading as ransomware

마이크로소프트 보안 인텔리전스 연구원들이 STRRAT 으로 추적되는 원격 액세스 트로이목마(RAT)을 확산시키는 악성코드 캠페인을 발견했다. 이 RAT 은 랜섬웨어 공격으로 위장하여 피해자의 데이터를 훔치도록 설계된 것으로 나타났다. 자바를 기반으로 한 STRRAT RAT 은 대규모 스팸 캠페인을 통해 배포되었으며, 악성코드는 실제로 파일을 암호화하지 않고 파일명에 .crimson 확장자를 추가한다.



[이미지 출처] https://twitter.com/MsftSecIntel/status/1395138347601854465

마이크로소프트에 따르면 이 캠페인의 배후에 있는 공격자들은 해킹된 이메일 계정을 사용하여 PDF 첨부파일로 위장한 이미지가 포함된 스팸 메시지를 발송했다. 이미지를 열면 악성코드가 STRRAT RAT 을 다운로드하기 위한 도메인으로 연결한다.

연구원들은 STRRAT 버전 1.5 가 이전보다 훨씬 난독화 및 모듈화되어 있음을 발견했다. 이 악성코드는 브라우저 비밀번호 수집, 원격 명령 및 PowerShell 실행, 키 입력 로깅 등 여러 기능을 지원한다. 2020 년 6 월 G DATA 에서 처음으로 STRRAT 을 발견한 당시 연구원들은 보고서를 발표해 다음과 같이 언급했다. “이 RAT 은 브라우저 및 이메일 클라이언트의 크리덴셜을 훔치는데 집중한다. 이는 Firefox, Internet Explorer, Chrome, Foxmail, Outlook, Thunderbird 를 포함한 브라우저 및 이메일 클라이언트를 지원한다.”

G DATA 의 전문가는 이 악성코드가 파일에 .crimson 확장자를 붙여 단순히 이름만 변경한다는 사실을 발견했다. '암호화'로 불리는 과정은 파일 끝에 .crimson 확장자를 붙여 단순히 이름을 변경하는 것이었으며 해당 파일을 더블클릭했을 때 실행할 수 없기 때문에 이 방법이 효력을 발휘할 가능성은 있다.

윈도우는 파일을 오픈할 때 확장자를 통해 알맞은 프로그램을 찾기 때문이다. 확장자를 제거할 경우 평소처럼 파일을 열 수 있다. 또한 이 RAT 의 클라이언트는 랜섬노트 템플릿을 포함하지 않으며 공격자는 show-msg 명령을 통해 원하는 메시지를 표시할 수 있으며 서버가 랜섬노트 템플릿을 제공할 수도 있다.

마이크로소프트의 연구원들은 관리자가 STRRAT 의 관련 지표 및 악성 행동을 찾는데 사용할 수 있는 헌팅 쿼리를 게시했다.

[출처]

https://securityaffairs.co/wordpress/118118/malware/strrat-rat-masquerading-ransomware.html

https://www.gdatasoftware.com/blog/strrat-crimson

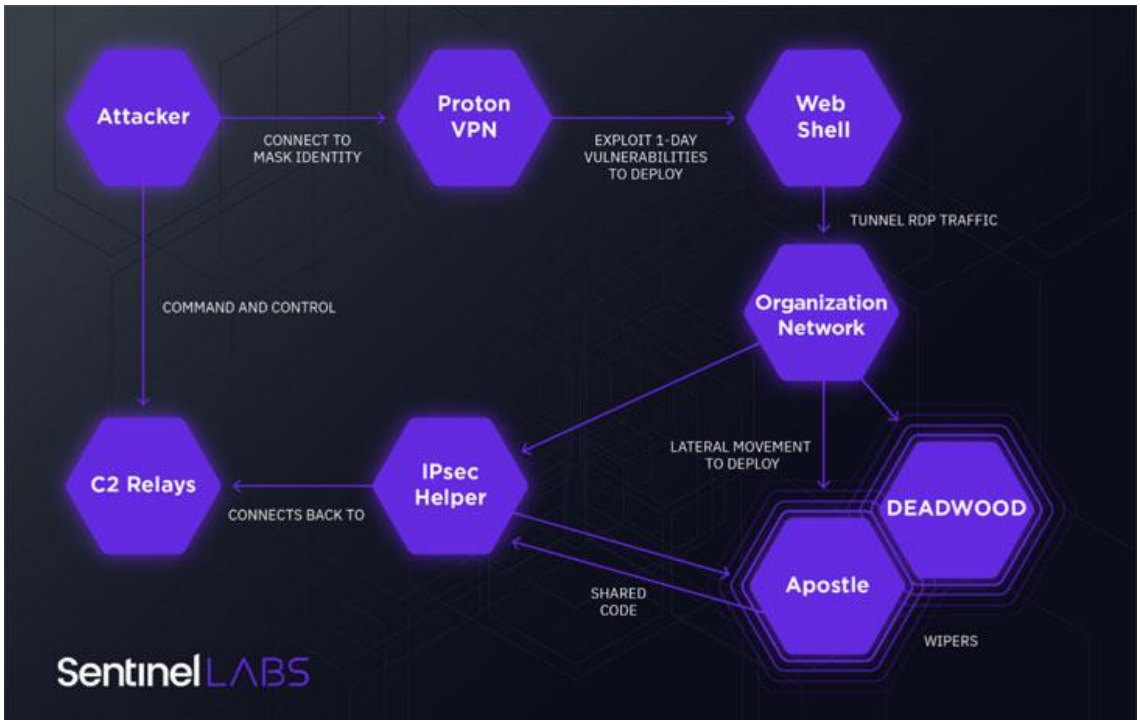
랜섬웨어로 위장한 데이터 와이퍼 악성코드, 이스라엘 기업 노려

Data Wiper Malware Disguised As Ransomware Targets Israeli Entities

2020 년 12 월부터 이스라엘 기업을 노리며 랜섬웨어로 위장해 파괴적인 데이터 와이핑 공격을 실행하는 새로운 스파잉 캠페인이 발견됐다. 보안 회사인 SentinelOne 은 이 캠페인이 “Agrius”라는 이름을 사용하는 이란 정부의 지원을 받는 공격자의 작업이라 밝혔다. 연구원들은 이에 대해 다음과 같이 언급했다. “이 공격은 언뜻 보면 랜섬웨어 공격으로 보이지만, 분석 결과 이스라엘 내 타깃을 노린 일련의 파괴적인 공격 중 사용된 새로운 와이퍼 변종인 것으로 나타났다. 이 공격의 배후에 있는 운영자는 금전을 노린 랜섬웨어 공격으로 위장해 자신의 공격을 숨겼다.”

이 그룹은 커스텀 .NET 악성코드인 ‘Apostle’을 사용하여 완전한 기능을 갖춘 랜섬웨어로 진화해 이전 와이퍼 기능을 대체하도록 했으나, Apostle 의 초기 버전에 존재하는 논리적 결함으로 인해 데이터가 지워지지 않아 공격 중 일부에서는 두 번째 와이퍼인 DEADWOOD(Detbosit)을 사용했다.

또한 Agrius 공격자는 데이터를 추출하거나 추가 악성코드를 배포하는데 사용될 수 있는 .NET 백도어인 IPsec Helper를 드롭했다. 공격자의 전략 또한 단순한 스파잉에서 피해자에게 암호화된 데이터를 복구해 주겠다고 약속하며 랜섬머니를 요구하는 것으로 변경되었다. 하지만 해당 데이터는 와이핑 공격을 통해 이미 파괴된 상태다.



[이미지 출처] https://assets.sentinelone.com/sentinellabs/evol-agrius

익명화를 위해 ProtonVPN 을 사용하는 것 이외에도, Agrius 공격 사이클은 웹 기반 애플리케이션에서 CVE-2018-13379 을 포함한 1-데이 취약점을 악용한다. 추가 진입점을 확보하고 해킹된 시스템에서의 원격 접속을 유지하고 임의 명령을 실행하기 위해 ASPXSpy 웹 셸을 배포하는 것이 목적이다.

연구원들은 이 공격에 대해 이란 정부와 관련이 있는 공격자들이 금전적 이득을 노리는 다른 랜섬웨어 그룹을 모방하기 위해 랜섬웨어 운영을 고려하고 있다는 증거라 밝혔다. “랜섬웨어 활동은 파괴적이고 효과적이며, 주 정부가 직접적인 비난을 받지 않고도 메시지를 전달할 수 있도록 한다. 다른 국가의 후원을 받는 공격자들 또한 유사한 전략을 사용하여 압도적인 영향을 미쳤다."

[출처]

https://thehackernews.com/2021/05/data-wiper-malware-disguised-as.html

https://assets.sentinelone.com/sentinellabs/evol-agrius

(주)이스트시큐리티

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