이스트시큐리티

보안 동향 보고서

No.131 2020.08

No.131 2020.08

이스트시큐리티 보안 동향 보고서

CONTENTS

01 악성코드 통계 및 분석 01-05

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

02 전문가 보안 기고 06-10

사이버전에도 보안 불감증 심각.. 대한민국 보안의 현주소

허위 결제 내역 정보를 이용한 국내 포털(NATE) 피싱메일 주의

03 악성코드 분석 보고 11-14

04 글로벌 보안 동향 15-26

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

7 월은 여느 때보다 피싱 및 스미싱 공격이 많이 발견된 달이었습니다.

"코로나19 7 월 추가 재난 지원금 신청" 활용한 스미싱 공격을 시작으로 "중앙행정기관 계정"을 노리는 피싱과 "국민건강검진 통지"를 사칭한 스미싱 공격이 주목할만한 이슈였습니다. 특히 국민건강검진 통지를 사칭한 스미싱 문자는 이전까지 발견됐던 스미싱과 조금 다른 양상을 보였습니다. 일반적인 스미싱 문자에 포함된 URL 이 사용자를 개인정보를 입력 받는 페이지로 리디렉션 했던 것과 다르게 이번에 발견된 공격은 클라우드 서비스를 활용하여 악성 앱 설치를 유도했습니다. 악성 앱은 구글 플레이 아이콘으로 위장했으며 백그라운드에서 계속 작동하며 감염된 스마트폰에서 수신되는 SMS 메시지를 탈취해 공격자에게 전달합니다. 공격자는 SMS 정보를 탈취하는 것 외에는 다른 악성 행위를 수행하지 않지만 공격자가 수집한 정보를 토대로 또 다른 2 차 공격을 수행할 가능성이 있기 때문에 사용자의 주의가 필요합니다. 사용자는 출처를 알 수 없는 문자 메시지에 포함된 URL 접속을 지양해야 하며 알약M 과 같은 신뢰할 수 있는 모바일 백신을 설치함으로써 피해를 최소화할 수 있습니다.

7 월 한 달 동안 국내에서 가장 주목할만한 악성코드는 "Emotet"입니다. Emotet 이 지난 2 월 이후 약 5 개월 만에 다시 공격을 개시했습니다. 최근 발견된 Emotet 변종은 피싱 메일의 신뢰성을 높을 목적으로 이메일의 첨부파일까지 훔치기 시작했습니다. 이러한 전략을 사용하는 악성코드는 Emotet 이 처음입니다. 뿐만 아니라 Emotet 은 TrickBot 과 QakBot 을 추가적으로 유포하며 뱅킹 트로이목마에서 봇넷 악성코드로 발전하였습니다. Emotet 의 활동은 7 월 한 달 동안 급격히 증가해 악성코드 분석 플랫폼에서 1 위를 차지하기도 하는 등 지속적인 모니터링이 필요합니다.

또한 Mac 운영 체제를 타깃으로 삼는 TheifQuest (EvilQuest) 랜섬웨어가 발견됐습니다. 토렌트 및 온라인 포럼을 통해 유포된 ThiefQuest 랜섬웨어는 타깃 파일을 암호화할 뿐만 아니라 감염시킨 호스트에서 키로거, 리버스 셸을 설치하고 가상 화폐 지갑과 관련된 파일을 탈취합니다. 다행히도 리버스 엔지니어링을 통해 TheifQuest 복호화 툴이 개발되어 암호화된 파일을 복구할 수 있게 됐습니다. 많은 사람들이 Mac 운영 체제가 악성코드로부터 안전하다고 생각하지만 최근 이러한 생각을 악용한 공격이 급속도로 증가하고 있습니다. 따라서 Mac 운영 체제 사용자들도 항상 악성코드 감염에 대한 경각심을 가지고 주의해야 합니다.

7 월은 6 월에 비해 APT 그룹의 공격이 두드러지지는 않았지만 라자루스(Lazarus) 그룹이 새로운 악성 프레임워크인 MATA 를 개발하여 VHD 랜섬웨어를 유포한 정황이 발견되었습니다. 라자루스는 MATA 프레임워크를 통해 소프트웨어 개발 기업, 인터넷 서비스 제공 업체, 전자 상거래 회사 등 다양한 업계의 기기를 해킹했습니다. 특히 MATA 프레임워크는 Window, Linux, Mac 운영 체제를 포함한 다양한 플랫폼을 공격할 수 있다는 점에서 중요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 7 월의 감염 악성코드 Top 25 리스트에서는 지난 3, 4, 5, 6 월에 1 위를 차지했던 Hosts.media.opencandy.com 이 7 월에도 동일하게 1 위를 차지했으며 지난달에 3 위를 차지했던 Misc.HackTool.AutoKMS 가 한 계단 상승해 2 위를 차지했다. 이번 달에는 Trojan.Downloader.Adload 및 3 건의 악성코드가 새롭게 Top 15 에 진입하였으며 그 외에는 지난달과 비슷한 양상을 보였다.

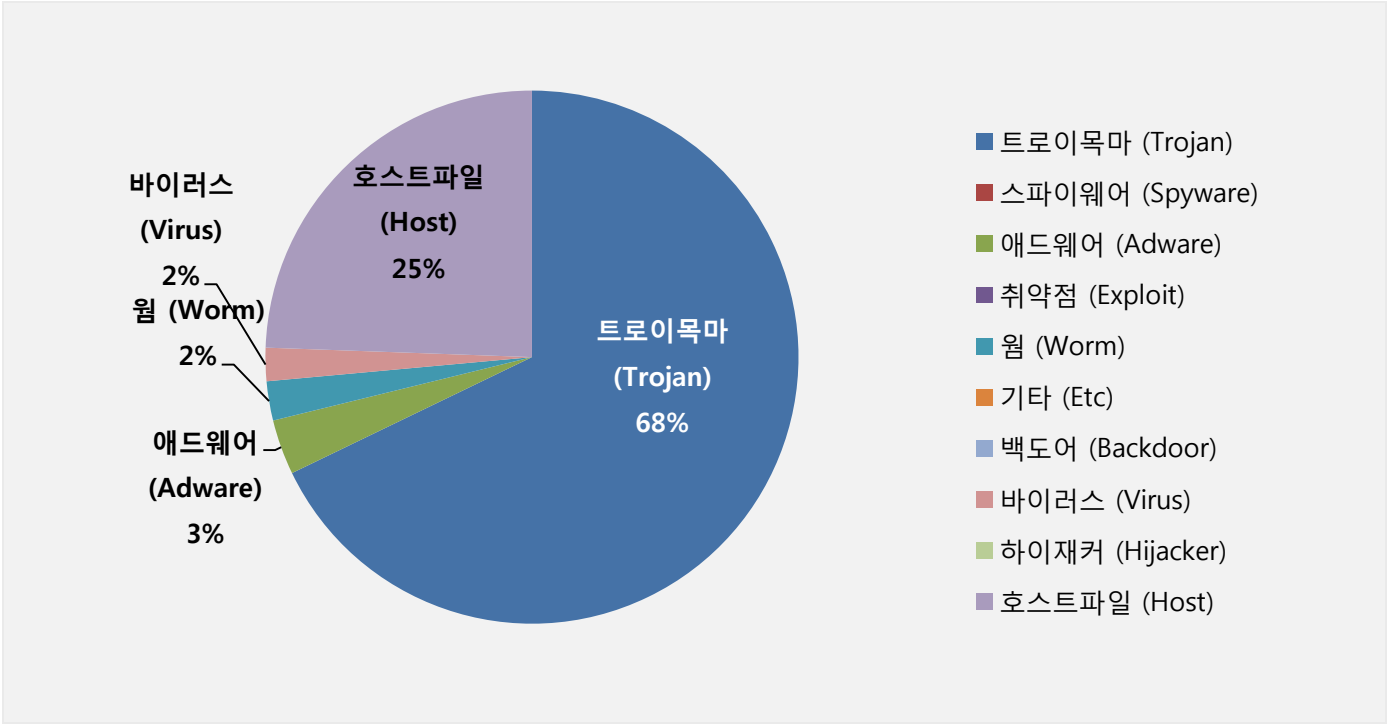
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	747,391
2	↑ 1	Misc.HackTool.AutoKMS	Trojan	418,290
3	↑ 2	Trojan.ShadowBrokers.A	Trojan	270,798
4	↑ 5	Misc.Keygen	Trojan	238,164
5	↓ 1	Trojan.Agent.gen	Trojan	194,176
6	-	Misc.HackTool.KMSActivator	Trojan	201,715
7	↓ 5	JS:Trojan.Cryxos.2745	Trojan	153,439
8	↑ 3	Gen:Variant.Razy.553929	Trojan	150,461
9	↑ 3	Trojan.Agent.EQGS	Trojan	133,735
10	New	Trojan.Downloader.Adload	Trojan	119,684
11	↓ 4	Misc.Riskware.TunMirror	Trojan	107,966
12	New	Gen:Varaiant.Adware.ConvertAd.134	Adware	102,130
13	New	Trojan.GenericKD.43365151	Trojan	86,588
14	-	Worm.ACAD.Bursted	Worm	72,740
15	New	Win32.Neshta.A	Virus	61,655

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 07 월 01 일 ~ 2020 년 07 월 31 일

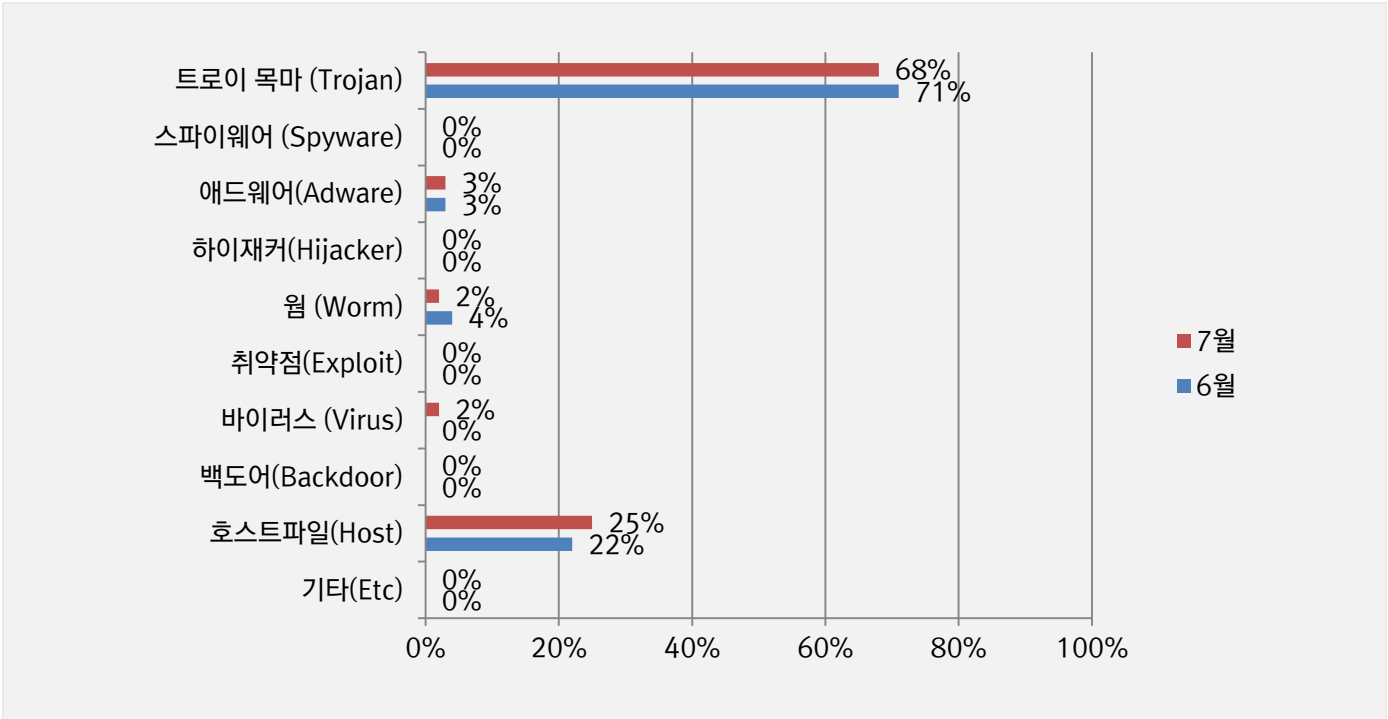
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 68%를 차지했으며 호스트파일(Host) 유형이 25%로 그 뒤를 이었다. 전반적으로 6 월에 비해 7 월의 전체 감염 건수는 4% 가량 소폭 감소하였다.



카테고리별 악성코드 비율 전월 비교

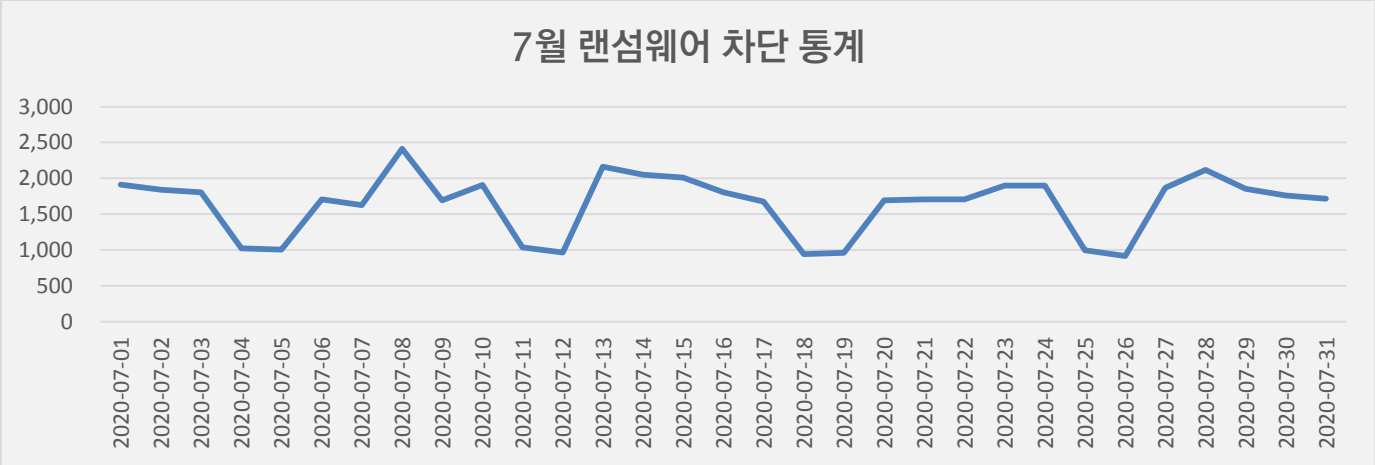
7 월에는 6 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율은 감소하였고, 호스트파일(Host) 유형 악성코드 비율이 약간 상승하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

7 월 랜섬웨어 차단 통계

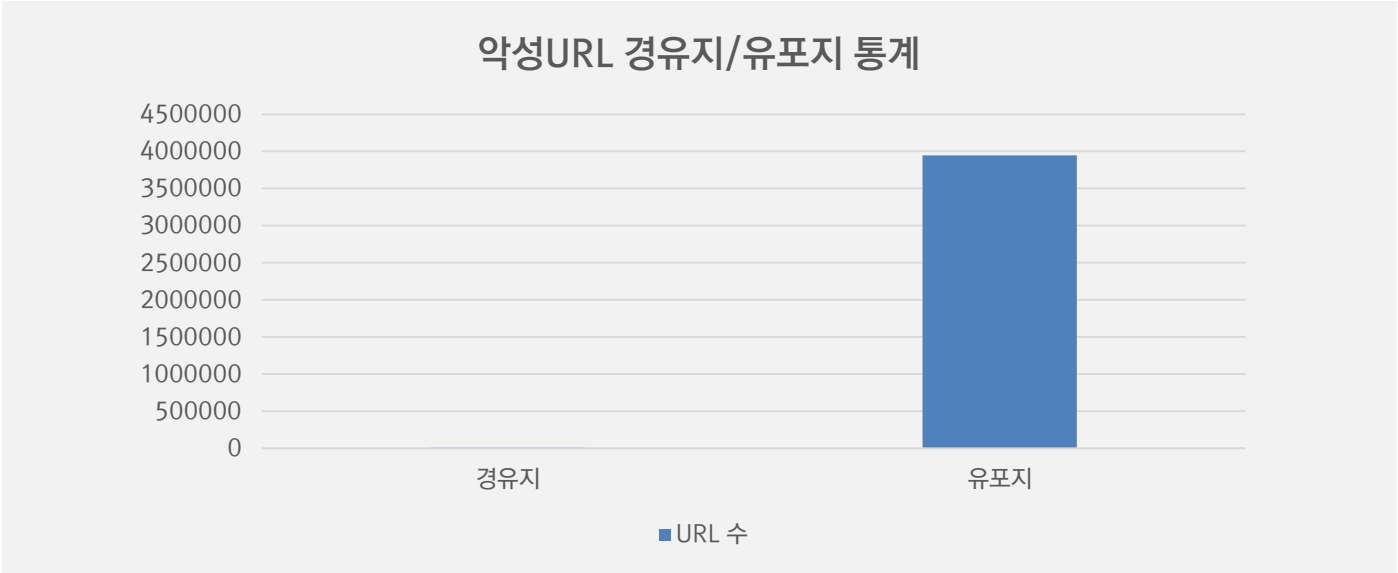
해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 7 월 1 일부터 7 월 31 일까지 총 50,653 건의 랜섬웨어 공격시도가 차단되었다. 6 월에 비해 랜섬웨어 공격건수는 약 4% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 7 월 한달간 총 3,953,744 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 6 월 한달 간 확인되었던 5,047,763 건의 악성코드 경유지/유포지 URL 수에 비해 약 21% 가량 감소한 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 봐주시기 바란다.



02
전문가 보안 기고

1. 사이버전에도 보안 불감증 심각.. 대한민국 보안의 현주소

2. 허위 결제 내역 정보를 이용한 국내 포털(NATE) 피싱메일 주의

1. 사이버전에도 보안 불감증 심각.. 대한민국 보안의 현주소

우리나라는 지난 2009 년 7 월 7 일 정부 기관을 포함한 여러 인터넷 사이트가 무차별 디도스 공격을 받아 서비스가 마비되는 초유의 사태를 경험했습니다. 이후에도 이 같은 사이버 공격은 계속 이어졌습니다. 지금 이 순간에도 수많은 지능형지속위협(APT) 공격의 중심에 서 있습니다.

보안업체 분석 보고서와 언론 보도를 통해 알려지는 사례가 있지만 이는 수많은 공격 가운데 극소수에 불과합니다. 그나마 알려진 내용도 대수롭지 않게 여기는 경우가 흔합니다. 공격이 얼마나 위험한지 체감하는 데 한계가 있는 것도 사실이지만 일각에선 보안 불감증이 심각한 수준이라는 지적이 제기됩니다.

보안 위협을 조기에 발견하고 탐지하면 다소 간단한 조치와 대응만으로 침해 사고 예방에 큰 도움이 됩니다. 위협 사각지대를 파악, 취약점을 빠르게 제거하는 데도 효과가 있습니다.

암세포를 조기 발견했을 때 '이건 암이 아니고 말기가 됐을 때 암이라 진단하겠다'고 정의한다면 암 치료가 더욱 어려워질 것입니다. 암세포가 전이되기 이전에 발견해 치료한다면 소요 시간과 치료비 등 여러 측면에서 효과를 볼 수 있을 것입니다.

사이버 위협도 마찬가지입니다. 하인리히 법칙처럼 대형 해킹 사고가 발생하기 전에 사소한 이상 징후나 경미한 이벤트가 여럿 나타날 수 있습니다. 이런 신호를 무시하거나 방관하고 있는 것은 아닌지 종합 점검을 해볼 필요가 있습니다.

우리나라는 정치, 외교, 안보, 통일, 국방 전·현직 종사자와 대북 분야에 종사하는 다양한 직종이 APT 주요 표적이 됩니다. 이런 경험을 통해 값비싼 교훈도 얻고 있습니다. 우리나라를 겨냥한 사이버 첩보 활동은 이미 일상화된 지 오래고, 위험성 역시 갈수록 증대되고 있습니다.

02 전문가 기고

사이버 보안 분야도 현실과 이상에 대한 괴리감이 존재하기 마련입니다. 결과 기반의 단편 접근 및 이해만으론 특정 정부와 연계된 APT 공격 조직이 너무 허술하고 단순해 보일 수도 있습니다. 그러나 실제 공격자 입장에서는 수없이 많이 진행하는 공격 시도의 일부이기 때문에 노출과 흔적에 대한 조심성이 부족할 수 있다는 공감대가 필요합니다.

정치·사회성 오해, 편견, 불신만으로 사이버 공격의 현실과 위험성을 제대로 인식하지 못한다면 그만큼 우리나라 안보의 앞날은 어두워집니다.

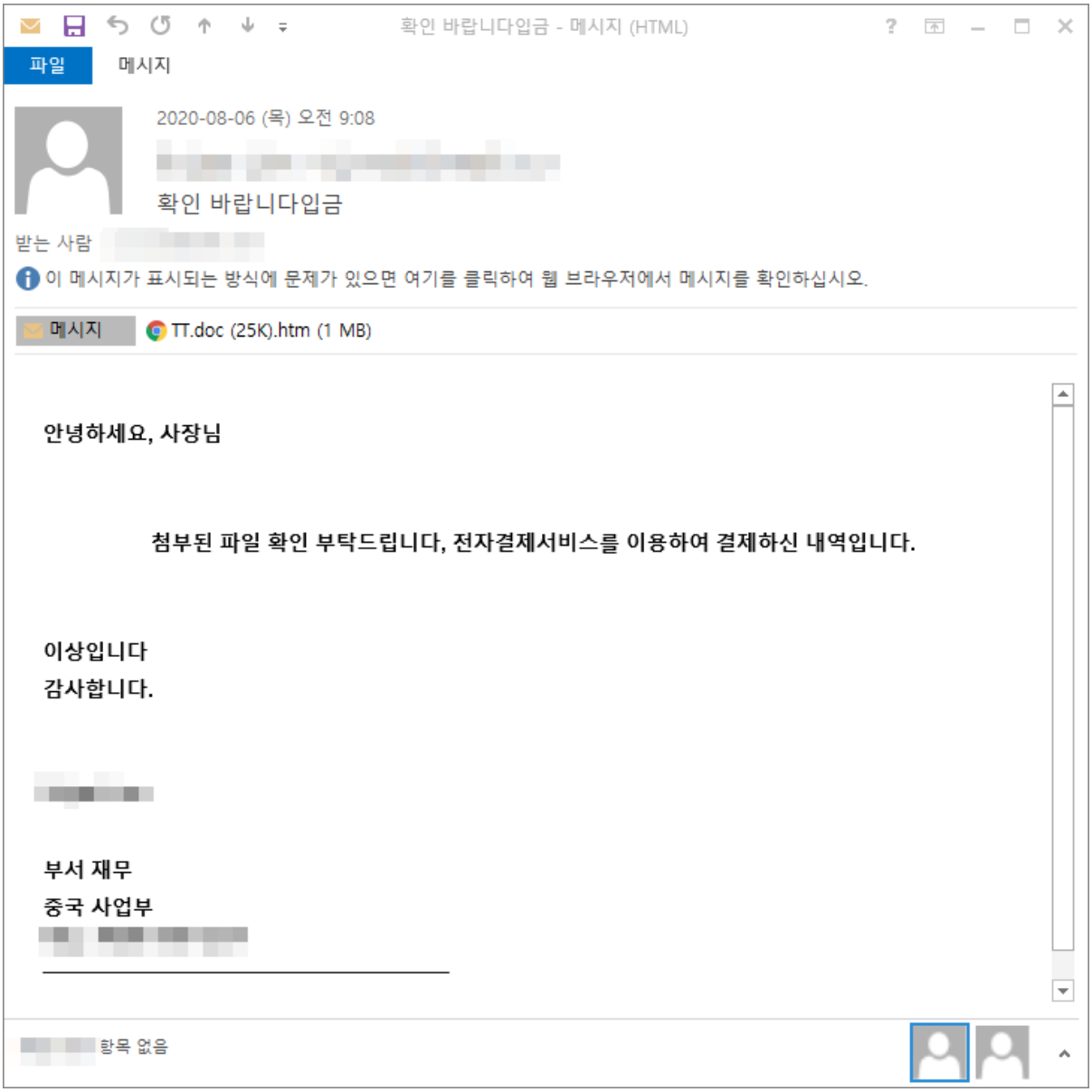
이솝우화에 등장하는 양치기 소년처럼 심심풀이로 "늑대가 나타났다"면서 거짓말로 혼란을 일으키는 것도 문제지만 늑대가 바로 옆까지 다가왔는데도 위협에 무감각하거나 아무도 대응하지 않는다면 더 큰 피해를 초래할 것입니다.

보안에는 편의와 속도에 반비례하는 공식이 있어 보안이 좋아질수록 편의와 속도는 낮아질 수 있습니다. 그러나 보안을 반복해야만 우리나라 안보를 지킬 수 있음을 잊지 말아야 합니다.

2. 허위 결제 내역 정보를 이용한 국내 포털(NATE) 피싱메일 주의

국내 대형 포털 사이트 계정을 노리는 피싱 메일이 발견되어 사용자들의 주의가 필요합니다.

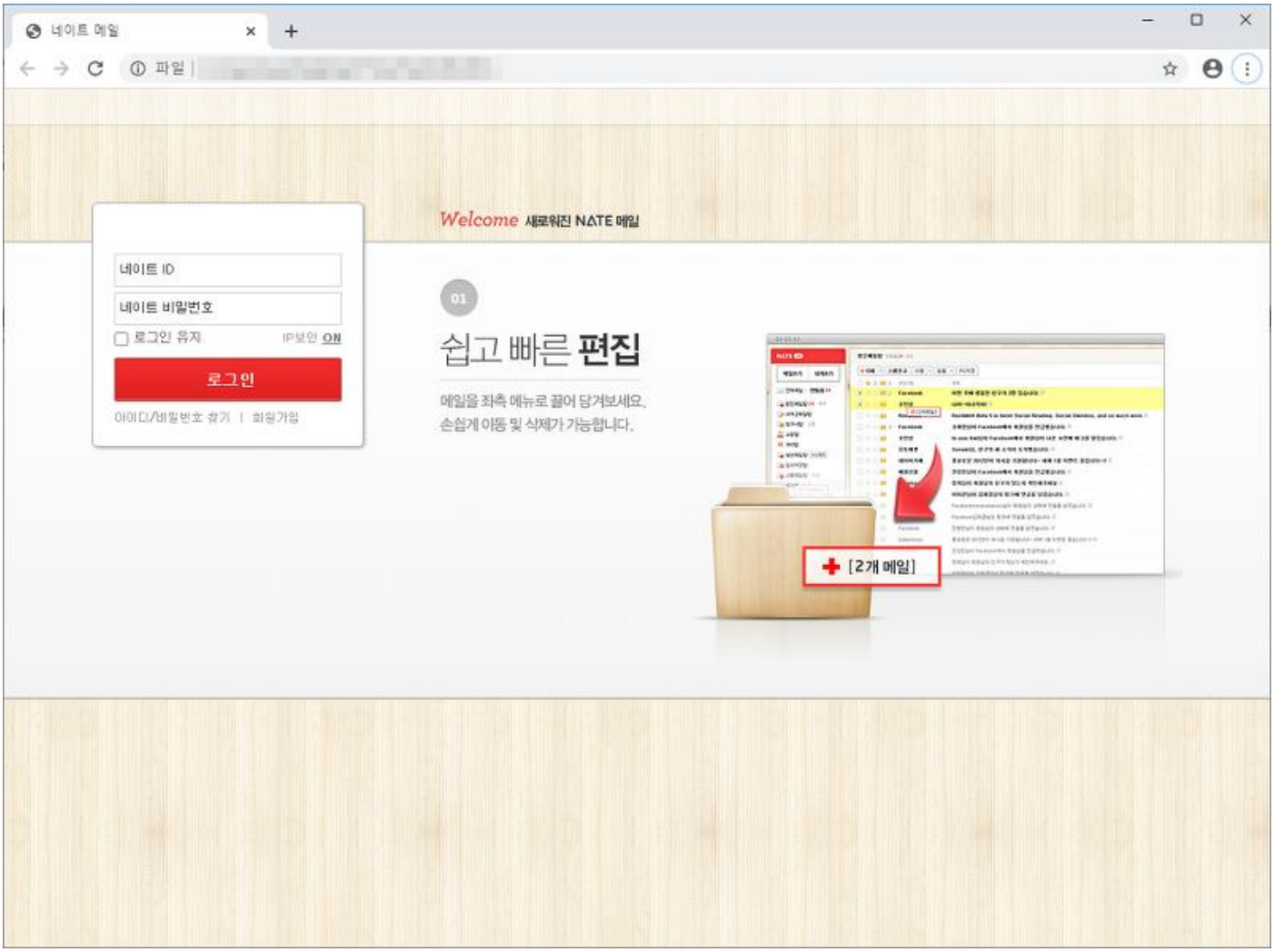
이번에 발견된 피싱 메일은 “확인 바랍니다 입금”라는 제목으로 전파되었으며, 전자결제 서비스를 이용하여 결제된 내역이 담긴 “TT.doc (25K).htm” 파일이 첨부되어 수신자의 첨부파일 실행을 유도하고 있습니다.



[그림 1] 국내 포털 사이트 계정을 노리는 피싱 메일 화면

02 전문가 기고

피싱 메일에 첨부된 파일은 “TT.doc”로 doc 의 문서처럼 보이지만 실제로는 “htm” 문서로 파일 실행 시 브라우저를 이용하여 피싱 페이지를 보여주게 됩니다.



[그림 2] 국내 포털 사이트 피싱 페이지 화면

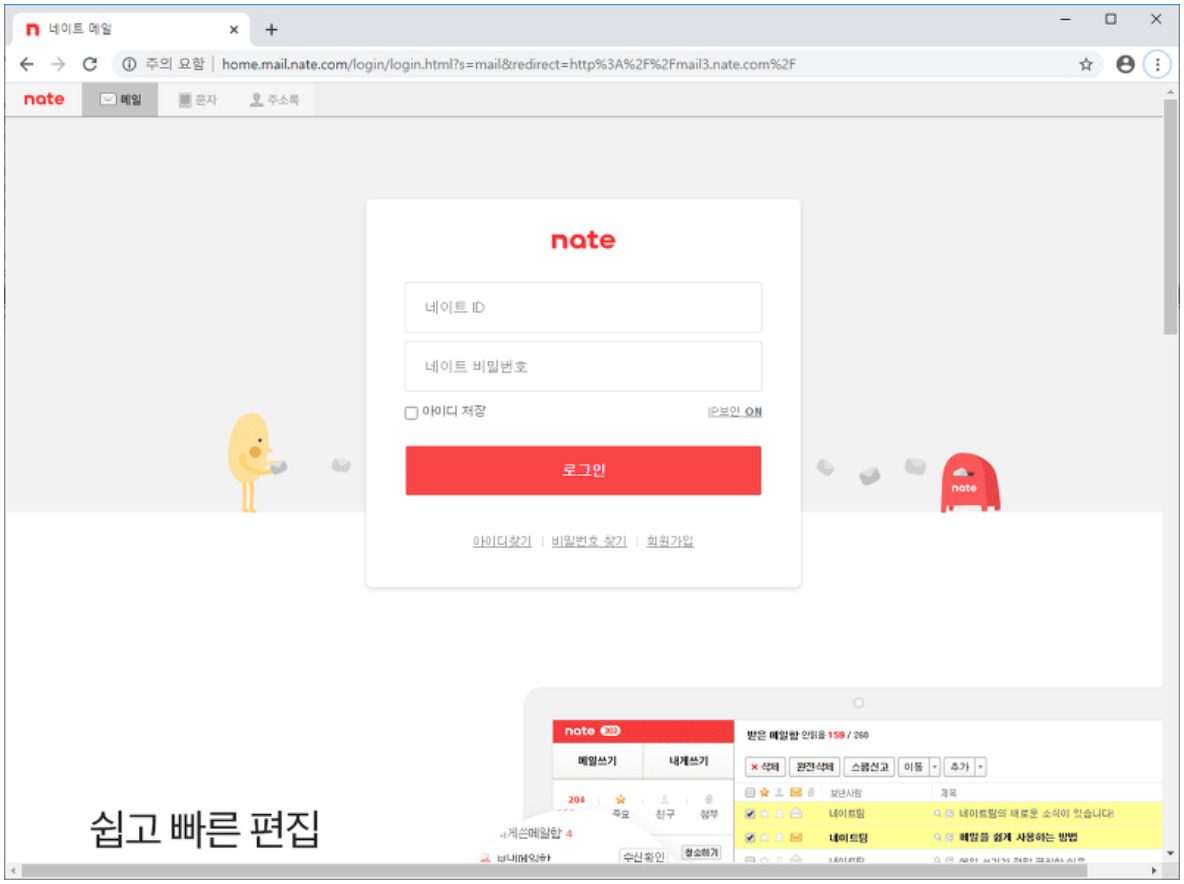
피싱 사이트에 계정과 비밀번호를 입력할 경우, 개인정보 수집 사이트로 입력된 개인정보가 전송되며 상세한 내용은 아래와 같습니다.

- 개인정보 수집 사이트
hxxps://proapform[.]com/obwork.php

- 개인정보 수집 서버 IP
205[.]134.255.185

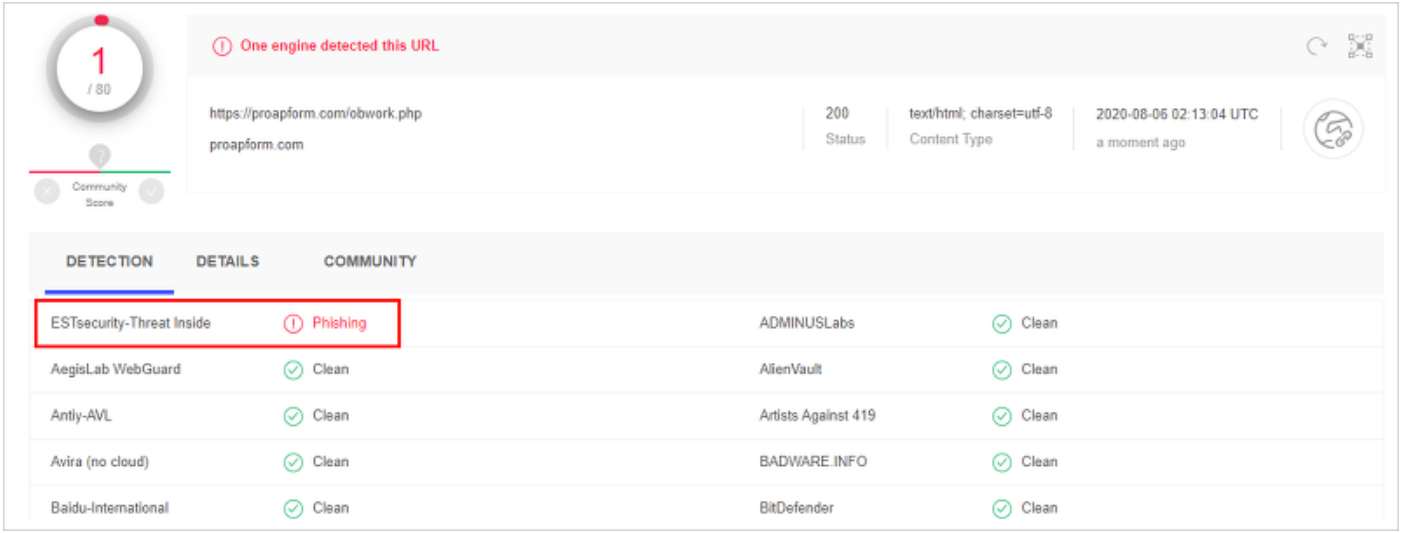
02 전문가 기고

입력된 개인정보 전송이 완료되면 정상적인 포털 사이트 로그인 페이지로 연결하기 때문에 사용자는 계정 정보가 유출된 사실을 알아차리기 어렵습니다.



[그림 3] 국내 포털 사이트 정상 로그인 페이지 화면

현재 이스트시큐리티 '쓰렛 인사이드(Threat Inside)'에서는 해당 개인정보 피싱 사이트를 아래와 같이 탐지하고 있습니다.

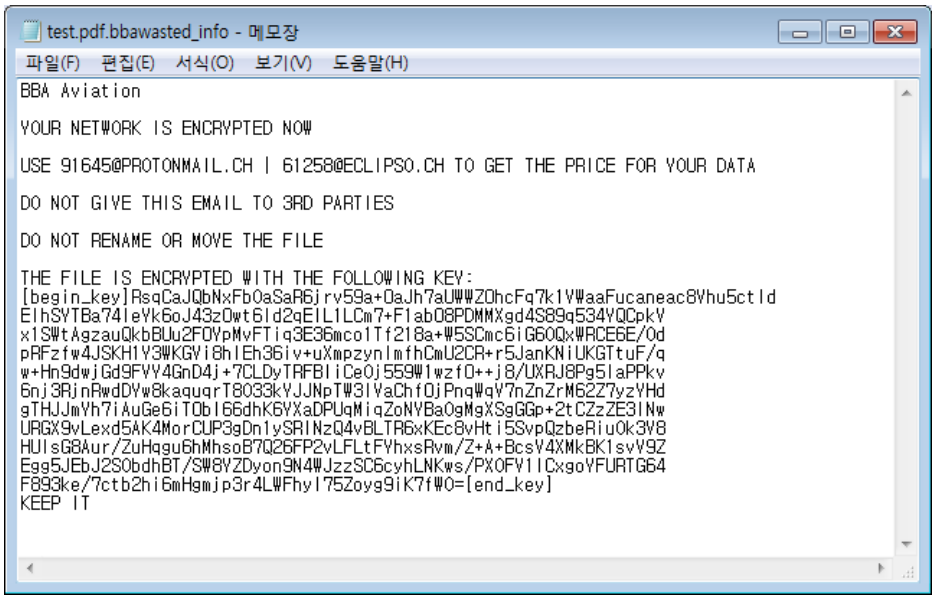


[그림 4] ESTsecurity-Threat Inside 개인정보 수집 사이트 탐지 화면

03
악성코드 분석 보고

[Trojan.Ransom.WastedLocker] 악성코드 분석 보고서

통칭 'WastedLocker'라 불리는 랜섬웨어는 기업을 대상으로 공격이 이루어지는 것으로 알려졌다. 실제 지난달 7 월 말 스마트워치와 웨어러블 기기 제조사인 가민(Gamin)이 랜섬웨어 공격을 받아 서비스 일부를 중단된 사례가 있다. 또한 이 랜섬웨어를 제작한 그룹은 뛰어난 기술력을 소유한 'Evil Corp' 또는 'TA505'로 해킹 그룹의 소행으로 알려져 있다.



[그림] 랜섬노트 화면

이 악성코드는 로컬에 존재하는 파일을 암호화시켜 감염자에게 파일 복호화를 대가로 돈을 받는 랜섬웨어의 한 종류다. 파라미터를 통하여 기능을 구별하여 실행하고 NTFS 의 ADS(Alternate Data Stream)을 이용하여 악성코드를 복사하고 은폐하는 특징이 있다.

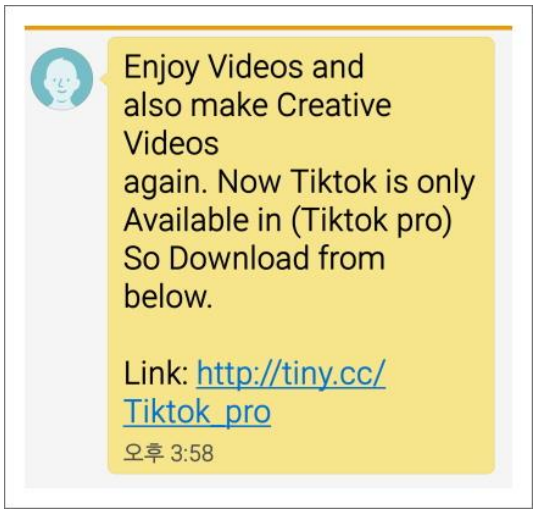
따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

현재 알약에서는 해당 악성 코드를 'Trojan.Ransom.WastedLocker' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Agent] 악성코드 분석 보고서

최근 인도에서 문자를 통한 악성 앱 공격이 화제가 됐었습니다. 이는 악성 앱 자체나 공격 방법이 화젯거리 라기 보다 인도 정부의 반중 정서에 따라 중국의 유명 SNS 앱인 Tiktok 을 인도에서 사용 금지하는 시점에 Tiktok 을 사칭한 공격이었기 때문이다.

특히 Tiktok 은 전체 사용자의 50% 이상이 인도 사용자일 정도로 인도에서의 인기는 대단하다. 공격자는 이런 이슈에 편승하여 Tiktok 앱으로 사칭한 악성 앱을 유포하였다. 이렇게 유포된 악성 앱은 의외로 별다른 악성 행위를 하지는 않으며 단지 광고 노출을 통해 금전적인 수익을 노린 것으로 추측된다.



[그림] 악성 앱이 보낸 문자

Trojan.Android.Agent 는 악성 앱을 유포하기 위해 스미싱을 활용하고 있다. 스미싱은 한국에서도 많이 활용되는 공격 방법이며 공격자 입장에서는 매우 유용한 공격 방법이기에 꾸준히 활용되고 있다.

사용자가 스미싱 공격을 통해 악성 앱을 설치하게 되면 공격자의 손에 스마트폰을 넘겨주는 것과 같다. 따라서 피해를 입기 전 예방하는 것이 가장 좋을 것이다.

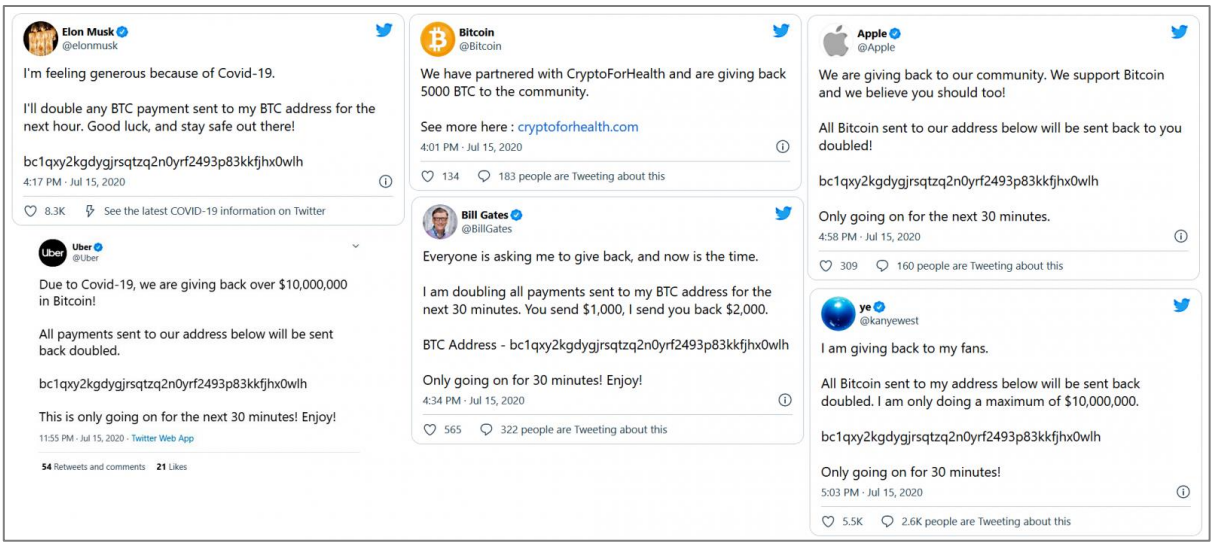
현재 알약M 에서는 해당 앱을 'Trojan.Android.Agent ' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

해커들, 관리자 툴 이용해 트위터 해킹 후 계정 훔쳐

Scammers hacked Twitter and hijacked accounts using admin tool

해커들이 내부 사용자 관리 툴 및 시스템에 접근 권한을 얻어내 유명 트위터 계정 수십 개를 하이재킹한 것으로 나타났다. 이후 이 계정은 가상 화폐 사기를 홍보하는데 악용되었다. 공격자는 유명 계정 다수를 통해 "비트코인을 보내면 2 배로 돌려주겠다"는 메시지를 게시했으며, 이를 통해 10 만 달러 이상을 벌어들일 수 있었다. 해커는 IT 기업과 임원, 연예인, 가상화폐 거래소 등 여러 유명 트위터 계정을 탈취하여 사기를 저질렀다. 공격자는 버락 오바마 전 미국 대통령, 조 비덴 전 미국 부통령 및 카니예 웨스트, 빌 게이츠, 킴 카다시안 등 유명 인사와 애플, 우버, 비트코인 등 기술 기업을 포함한 여러 트위터 계정을 탈취하는데 성공했다.



[그림 1] 해커 포럼 광고

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

이 사고가 발견된 직후, 트위터는 모든 검증된 계정에서 트윗을 게시하거나 비밀번호를 재설정하는 것을 차단했다.
3 시간 후, 트위터는 해당 계정에서 트윗 기능이 복구되었으나 조사가 진행됨에 따라 의도치 않게 다시 차단될 수 있다고 밝혔다.

[그림 2]

[출처] https://twitter.com/jack/status/1283571658339397632

계정 하이재킹에 내부 관리 툴 사용돼

트위터 측은 이 사고에 대해 조사한 후 다음과 같이 밝혔다.
"공격자가 내부 시스템과 툴에 대한 접근 권한이 있는 직원 중 일부를 성공적으로 해킹한 후 소셜 엔지니어링 공격을 실행한 것을 발견했다."
"공격자는 이 접근 권한을 악용하여 많은 유명 계정(검증된 계정 포함)을 제어하여 그들을 대신하여 트윗을 게시했다. 공격자가 추가로 실행한 다른 공격이 있는지, 어떤 정보에 접근했는지에 관한 조사를 진행 중이다. 준비되는 대로 추가로 정보를 공유해 드리도록 하겠다."

트위터 팀은 도용된 트위터 계정을 즉시 잠금 상태로 전환했으며 가상화폐 사기 트윗 또한 삭제했다.
"해킹된 계정을 잠금 상태로 전환했으며, 안전하다고 판단될 경우에만 해당 계정의 실제 주인이 다시 접속할 수 있도록 복구할 예정이다."
"조사가 진행되는 동안 내부적으로는 내부 시스템 및 툴에 대한 접근을 제외하는 상당한 조치를 취했다. 조사가 진행됨에 따라 추가로 정보를 공개하도록 하겠다."

[그림 3]

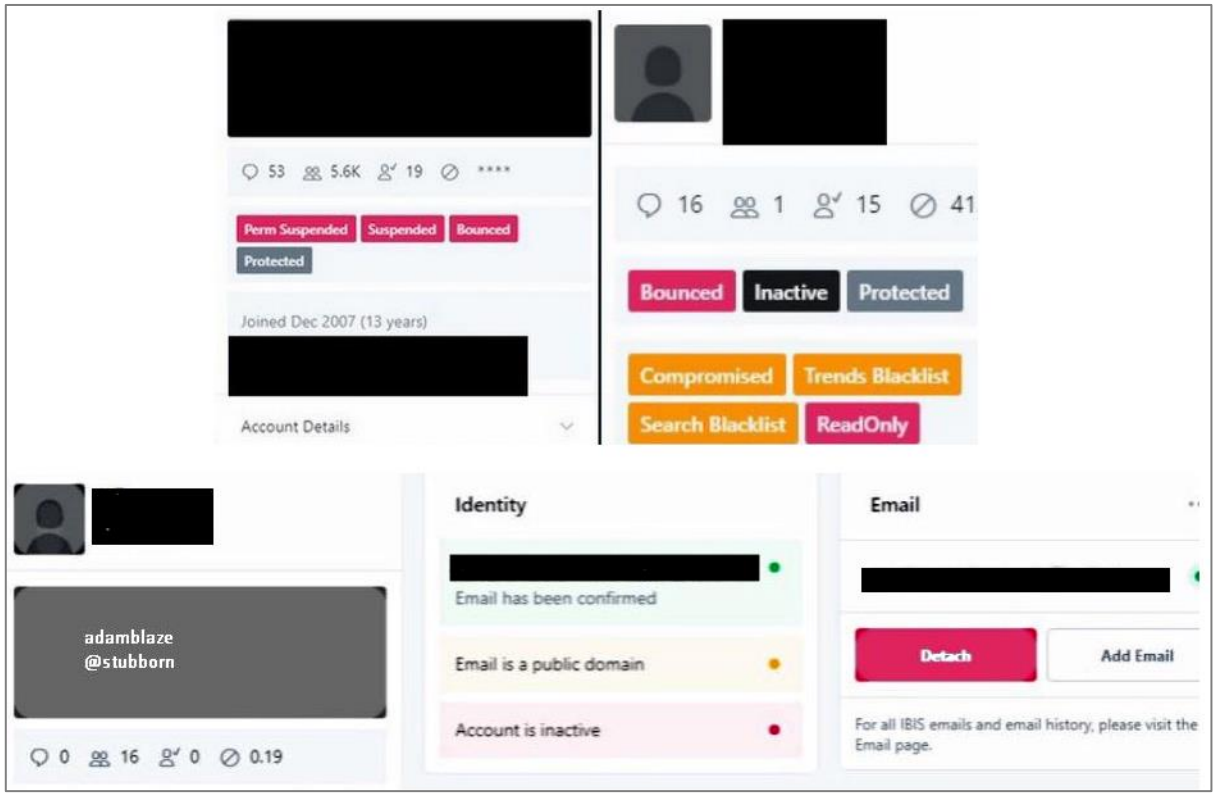
[출처 https://twitter.com/TwitterSupport/status/1283591851572973573

트위터 내부 직원의 소행일까?

트위터 측은 공격자가 계정을 탈취하는데 내부 직원이 협력한 사실이 있는지, 공격자가 마음대로 관리 툴에 접근하도록 방법을 제공했는지, 아니면 공격자가 직원들 몰래 트위터의 내부 툴 제어 권한을 얻어낸 것인지는 아직까지 확인하지 못했다. 내부 툴 인터페이스는 데이터 유출 모니터링 및 예방 서비스인 Under The Breach 및 다른 계정 다수의 공격을 받아 트위터에 유출된 것으로 나타났다.

공격자들이 내부 사용자 관리 패널의 스크린샷을 공개한 직후, 트위터의 직원은 이를 제거한 후 "이 트윗은 트위터의 규칙을 위반했다."라는 메시지를 남겼으며 해당 계정을 일시적으로 차단했다.

Under the Breach는 해커들이 그들이 저지른 범죄에 대해 자랑하며, 계정 하이재커 및 SIM 스와퍼 사이에서 유명한 OGUsers 해커 포럼에서 홍보된 Discord 서버에 트위터 패널 스크린샷을 공유했다고 밝혔다.



[그림 4] 트위터 관리자 패널

이 사건에는 내부 직원이 개입했는지 알 수 없지만, 트위터에서 인재가 발생한 것은 이번이 처음은 아니다. 이전에도 트위터 전 직원이 내부 시스템을 사용하여 "사우디의 비평가 및 트위터 사용자 수천 명"의 정보를(이메일 주소, IP 주소, 생년월일) 수집해 사우디아라비아 왕국에 공유한 혐의로 고소당한 적이 있다.

트위터 계정 다수에 대한 공격이 발생하자 구글 또한 유명 회사 및 개인 트위터 계정의 트윗을 표시하는 검색 페이지를 제거해 공격이 노출되는 범위를 축소시켰다.

또한 모든 사용자들이 비트코인 주소와 유사한 문자열을 포함한 트윗을 게시하지 못하도록 차단했다. 이에 파일 해시, Git 파일 경로 등 유사한 문자열 형식 또한 차단되어 일부 보안 분석가와 코드 개발자가 업무에 방해를 받았다. 그리고 금일 트위터는 해커가 사용자의 비밀번호에 접근했다는 증거를 찾을 수 없었다고 밝혔다. 따라서 어제 사고로 인해 사용자의 비밀번호를 변경할 계획은 없다고 전했다. 또한 아직까지 조사가 진행 중이며 미 법 집행 기관 또한 이 사건을 조사하고 있다고 전했다.

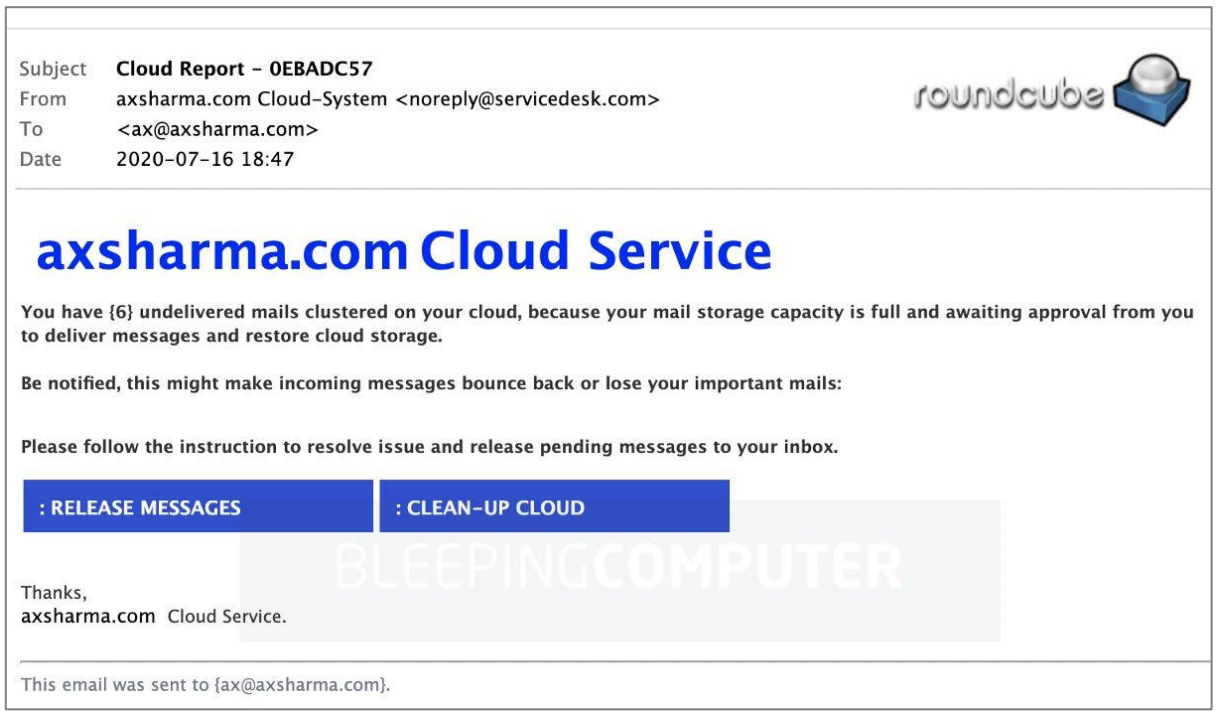
[출처] https://www.bleepingcomputer.com/news/security/scammers-hacked-twitter-and-hijacked-accounts-using-admin-tool/
https://www.zdnet.com/article/twitter-no-evidence-hackers-accessed-user-passwords/
https://securityaffairs.co/wordpress/105970/hacking/high-profile-twitter-bitcoin-scam.html

엔터프라이즈 클라우드 서비스 3 곳을 악용하는 새로운 피싱 캠페인 발견

New phishing campaign abuses a trio of enterprise cloud services

사용자의 로그인 자격 증명을 훔치기 위해 엔터프라이즈 클라우드 서비스인 마이크로소프트 Azure, Dynamics, IBM Cloud 3 곳을 악용하는 새로운 피싱 캠페인이 발견되었다.

Bleeping Computer 는 최근 헬프 데스크에서 전송한 것으로 가장했으며 "servicedesk.com"라는 기업의 실제 IT 헬프 데스크 도메인에서 사용하는 것과 유사한 단어를 사용하는 새로운 피싱 캠페인을 발견했다.
피싱 메일은 직장 내 이메일 보안 제품 및 스팸 필터에서 종종 발송되는 대기열에 걸린 메시지를 "해제"할 것을 요구하는 "검역된 메일" 알림을 모방했다.


Subject Cloud Report - 0EBADC57
From axsharma.com Cloud-System <noreply@servicedesk.com>
To <ax@axsharma.com>
Date 2020-07-16 18:47

roundcube

axsharma.com Cloud Service

You have {6} undelivered mails clustered on your cloud, because your mail storage capacity is full and awaiting approval from you to deliver messages and restore cloud storage.

Be notified, this might make incoming messages bounce back or lose your important mails:

Please follow the instruction to resolve issue and release pending messages to your inbox.

: RELEASE MESSAGES : CLEAN-UP CLOUD

BLEEPINGCOMPUTER

Thanks,
axsharma.com Cloud Service.

This email was sent to {ax@axsharma.com}.

[그림 1] IT 지원 센터에서 온 것으로 위장한 피싱 이메일

이 이메일의 송신자는"noreply@servicedesk.com"으로 표시되어 있었다. 이메일 송신자 부분은 쉽게 스푸핑이 가능하지만, 이 피싱 캠페인의 메일 헤더는 해당 이메일이 실제 이 도메인을 통해 전송된 것으로 표시된다. 이메일 헤더에서 확인할 수 있듯 이 피싱 이메일은 중개 "cn.trackhawk.pro" 도메인을 통해 전송되었으나 발신 도메인은 명백히 "servicedesk.com"다.

```
Return-Path: <noreply@servicedesk.com>
Delivered-To: ax@axsharma.com
Received: from server198.web-hosting.com
        by server198.web-hosting.com with LMTP
        id kMutCmcWEV/rawEAGw0NTw
        (envelope-from <noreply@servicedesk.com>)
        for <ax@axsharma.com>; Thu, 16 Jul 2020 23:09:27 -0400
Return-path: <noreply@servicedesk.com>
Envelope-to: ax@axsharma.com
Delivery-date: Thu, 16 Jul 2020 23:09:27 -0400
Received: from cn.trackhawk.pro ([66.23.232.62]:59939)
        by server198.web-hosting.com with esmtps  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        (Exim 4.93)
        (envelope-from <noreply@servicedesk.com>)
        id 1jwGkY-000PG6-UL
        for ax@axsharma.com; Thu, 16 Jul 2020 23:09:27 -0400
Received: from servicedesk.com ([104.37.188.73]) by trackhawk.pro with
 MailEnable ESMTPA; Thu, 16 Jul 2020 15:47:24 -0700
From: "axsharma.com Cloud-System" <noreply@servicedesk.com>
To: ax@axsharma.com
Subject: Cloud Report - 0EBADC57
Date: 16 Jul 2020 15:47:24 -0700
Message-ID: <20200716154724.97E50257DBC79111@servicedesk.com>
MIME-Version: 1.0
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

[그림 2] 피싱 이메일 메시지의 오리지널 헤더

대부분의 이메일 스푸핑 시나리오에서 “From:” 이메일 도메인과 맨 아래 “Received:” 헤더에 리스팅된 도메인이 일치하지 않을 경우 위험한 것으로 간주된다. 이 캠페인에서는 “From:”에 사용된 도메인인 “servicedesk.com”이 마지막 “Received:” 헤더에 리스팅된 도메인과 일치해 더욱 쉽게 스팸 필터를 우회할 수 있게 된다.

```
Return-Path: <noreply@servicedesk.com>
Delivered-To: ax@axsharma.com
Received: from server198.web-hosting.com
        by server198.web-hosting.com with LMTP
        id kMutCmcWEV/rawEAGw0NTw
        (envelope-from <noreply@servicedesk.com>)
        for <ax@axsharma.com>; Thu, 16 Jul 2020 23:09:27 -0400
Return-path: <noreply@servicedesk.com>
Envelope-to: ax@axsharma.com
Delivery-date: Thu, 16 Jul 2020 23:09:27 -0400
Received: from cn.trackhawk.pro ([66.23.232.62]:59939)
        by server198.web-hosting.com with esmtps  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        (Exim 4.93)
        (envelope-from <noreply@servicedesk.com>)
        id 1jwGkY-000PG6-UL
        for ax@axsharma.com; Thu, 16 Jul 2020 23:09:27 -0400
Received: from servicedesk.com ([104.37.188.73]) by trackhawk.pro with
 MailEnable ESMTPA; Thu, 16 Jul 2020 15:47:24 -0700
From: "axsharma.com Cloud-System" <noreply@servicedesk.com>
To: ax@axsharma.com
Subject: Cloud Report - 0EBADC57
Date: 16 Jul 2020 15:47:24 -0700
Message-ID: <20200716154724.97E50257DBC79111@servicedesk.com>
MIME-Version: 1.0
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

[그림 3] 피싱 이메일 메시지의 오리지널 헤더

이 헤더는 아래 두 가지 중 하나의 경우를 나타낸다.

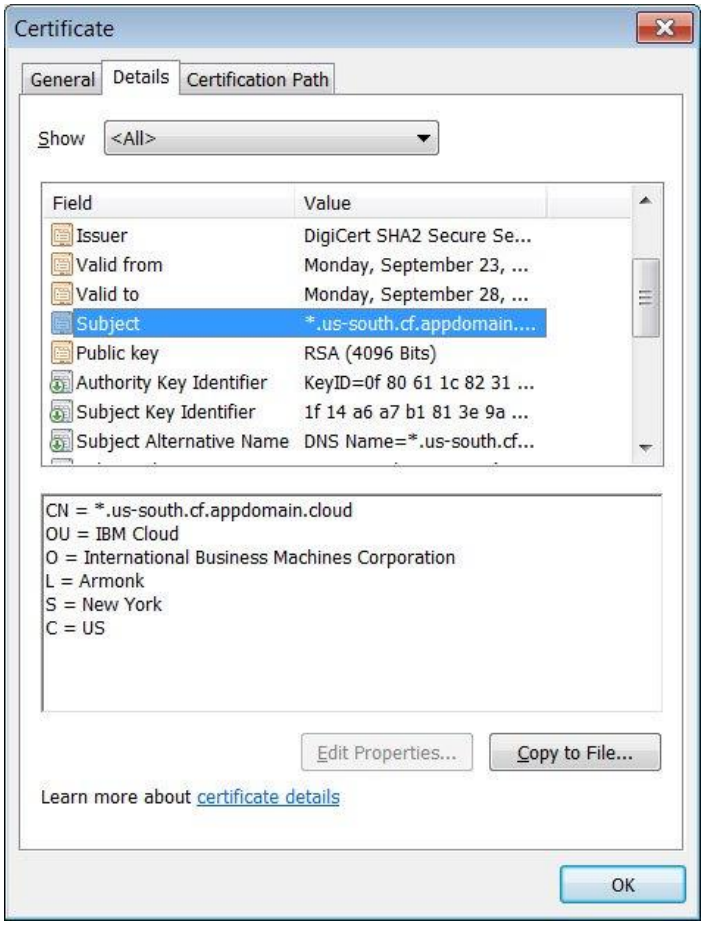
-"servicedesk.com" 메일 서버가 해킹되어 공격자가 해당 서버를 통해 이메일을 보냄

- 공격자는 "cn.trackhawk.pro" 도메인을 통해 이메일을 보냈지만 위조된 "Received: from servicedesk.com ..." 헤더를 아래에 주입해 "From:" 도메인과 매치되도록 하여 신뢰도를 높임

흥미롭게도 "Received: from servicedesk.com ([104.37.188.73])" 내 나열된 IP 주소에 ping 을 보내면 시간 초과 결과가 반환되어 이 서버가 활성화되어 있지 않다는 것을 의미한다. 하지만 "cn.trackhawk.pro" IP (66.23.232.62)는 ping 에 적절한 답변을 반환하기 때문에 위에 언급된 시나리오 중 2 번일 가능성이 높다. 또한 "servicedesk.com" 도메인에 대한 DMARC, DKIM, SPF 검증이 없기 때문에 스패머가 이 도메인을 악용할 수 있도록 허용하게 된다.

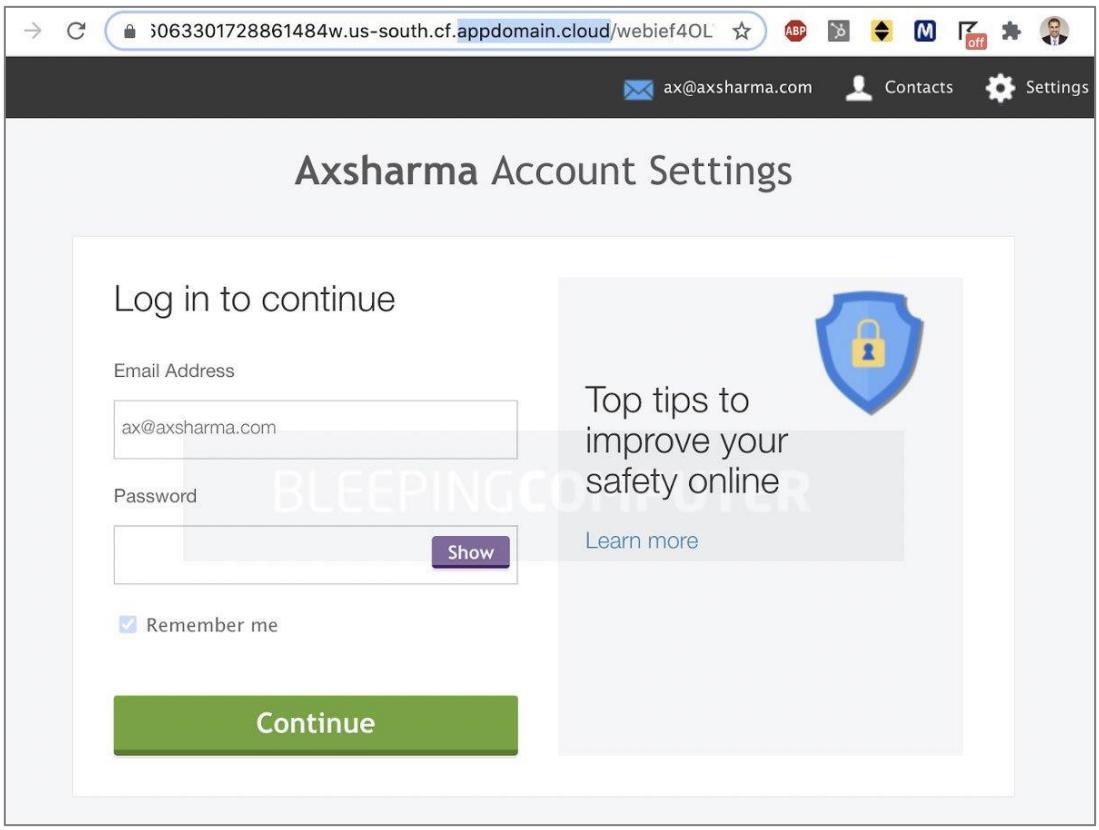
마이크로소프트와 IBM 도메인, 합법성 더해

IBM 클라우드 호스팅, 마이크로소프트, Azure, Dynamics 와 같이 잘 알려진 엔터프라이즈 솔루션을 사용하여 피싱 랜딩 페이지를 호스팅하는 이유는 캠페인에 합법성을 더하기 위함이다. Azure (windows.net) 또는 IBM 클라우드에서 호스팅되는 도메인은 이 회사의 이름을 포함하는 무료 SSL 인증서를 얻을 수 있기 때문에 더욱 합법적으로 보일 수 있다.



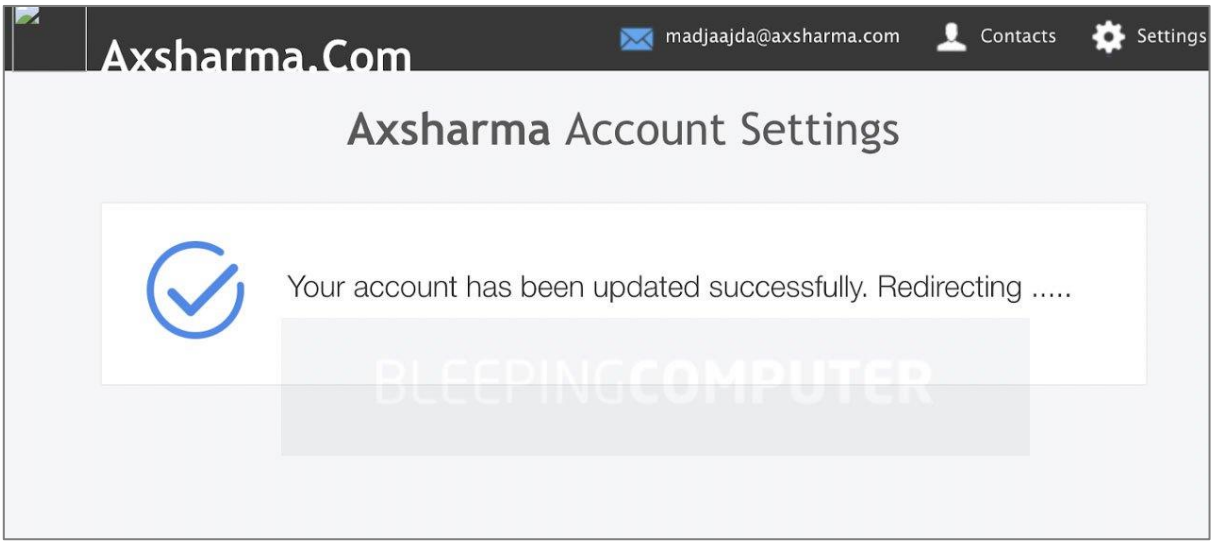
[그림 4] IBM 클라우드 인증서

피싱 이메일에는 “RELEASE MESSAGES” 또는 “CLEAN-UP CLOUD” 라벨이 붙은 버튼이 있으며 클릭할 경우 사용자를 합법적인 마이크로소프트 Dynamics 365 URL 로 이동시킨다. 이후 이 URL 은 피싱 랜딩페이지를 호스팅하기 위해 사용자를 IBM 의 Cloud Foundry 배포에 사용되는 IBM 클라우드 도메인인 cf.appdomain.cloud 로 이동시킨다.



[그림 5] IBM 클라우드 서버의 랜딩 페이지

이 랜딩 페이지는 사용자가 너무 취약한 “테스트” 비밀번호를 입력할 경우 “잘못된 비밀번호 입니다!”라는 에러를 표시하도록 설계되었다. IBM 클라우드 비밀번호에 길이와 복잡도가 적절한 비밀번호를 입력할 경우 사용자는 마이크로소프트 Azure 의 호스팅 도메인인 windows.net 의 설정 업데이트 호스트를 확인하는 또 다른 가짜 페이지로 이동된다.



[그림 6] Azure windows.net 도메인의 파이널 랜딩 페이지

이 악성 페이지는 사용자를 결국 그들의 이메일 주소 도메인과 관련된 웹사이트로 이동시킨다. 이 피싱 캠페인의 경우 최종 목적지는 “axsharma.com”이었다. 피싱 이메일은 기업 및 개인에게 늘 익숙하지만 데이터 도난 및 전사적 랜섬웨어 공격과 같은 심각한 결과를 초래할 수 있다. 공격자들이 피싱 공격에 합법성을 더하고 무료 SSL 인증서를 제공하기 위해 합법적인 클라우드 인프라를 악용하는 피싱 캠페인이 증가하는 추세다. 이렇듯 공격을 더욱 복잡하게 만들어 스팸 필터와 보안 제품을 우회 가능할 수 있어 정교한 보안 시스템의 필요성이 더욱 커지게 된다.

[출처] https://www.bleepingcomputer.com/news/security/new-phishing-campaign-abuses-a-trio-of-enterprise-cloud-services/

Sodinokibi 랜섬웨어, Telecom Argentina 의 컴퓨터 18,000 대 감염시켜

Sodinokibi ransomware infected 18,000 computers at Telecom Argentina

아르헨티나의 최대 규모 인터넷 서비스 제공 업체 중 하나인 Telecom Argentina 가 랜섬웨어의 공격을 받은 것으로 나타났다. 랜섬웨어 운영자들은 지난 주말 동안 컴퓨터 약 18,000 대를 감염시켰으며 랜섬머니로 750 만 달러를 요구하고 있다.

이 사고는 지난 토요일인 7 월 18 일 발생했으며 회사 업무에 치명적인 영향을 끼쳤다. 공격자들은 먼저 회사 네트워크로의 접근 권한을 얻어 내부 도메인 관리자 권한을 탈취해 만 대가 넘는 컴퓨터를 감염시킬 수 있었다.

이 사고로 인해 해당 ISP 고객의 연결성에는 문제가 발생하지 않았다. 유선 통신 및 케이블 TV 서비스 또한 영향을 받지 않았다. Telecom Argentina 가 운영 중인 많은 웹사이트가 이 공격으로 인해 다운되었다. 보안 연구원인 German Fernandez 는 이 공격이 Sodinokibi 랜섬웨어의 소행인 것으로 추측했다.

[그림 1]

[출처 https://twitter.com/1ZRR4H/status/1284947544171307010

내부 IT 직원이 공격을 발견한 즉시 회사는 직원들에게 내부 VPN 네트워크에 연결하지 말고 수상한 압축 파일이 첨부된 이메일을 열지 말 것을 경고했다.

Sodinokibi(REvil) 랜섬웨어 그룹은 다크웹 지불 포털에 Telecom Argentina 전용 페이지를 만들었다. 해당 페이지에서는 109345.35 모네로 코인을(약 90.2 억원) 랜섬머니로 요구하고 있었다. 이 글을 쓰고 있는 시점에서 해커는 아직까지 Telecom Argentina 의 정보를 다크웹 유출 사이트에 게시하지 않은 상태다. 이 랜섬웨어 공격자들은 Telecom Argentina 에서 3 일 내 랜섬머니를 지불하지 않을 시 가격이 2 배로 증가한다고 위협하고 있었다. Sodinokibi 운영자들은 과거에는 Pulse Secure 과 Citrix VPN, 엔터프라이즈 게이트웨이 시스템을 침입 지점으로 활용했다.

Sodinokibi 랜섬웨어의 공격을 받은 ISP 업체는 Telecom Argentina 가 처음은 아니다. 이들은 지난 5 월 스리랑카 텔레콤의 시스템을 감염시켰다. 지난 7 월 초, 또 다른 ISP 인 Orange SA 또한 랜섬웨어 공격을 당해 기업 고객 20 명의 데이터를 노출시켰다.

[출처] https://securityaffairs.co/wordpress/106147/cyber-crime/telecom-argentina-revil-ransomware.h

(주)이스트시큐리티

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