

이스트시큐리티 보안 동향 보고서

No.124 2020.01



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	06-14
	Apple iPhone 분실 관련 스미싱 메시지 주의!	
	크리덴셜 스테핑(Credential Stuffing) 공격으로 인한 클라우드 보안 주의!	
03	악성코드 분석 보고	15-17
04	글로벌 보안 동향	18-23

01

악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2019년 12월에도 전통적인 공격자 그룹인 코니, 비너스락커, 김수키, TA505 조직들이 다양한 주제를 활용하여 사용자를 현혹시키는 스피어피싱 이메일을 통해 APT 공격을 시도하는 정황이 여러차례 포착이 되었습니다. 수 백 개의 대한민국 제조업체를 메인 타겟으로 하는 ‘강남 인더스트리얼 스타일(Gangnam Industrial Style) 캠페인’이라 명명된 APT 공격이 발견되기도 하였습니다.

또한, 12월은 이전과 비교했을 때 유독 확장 프로그램 / 애드온 프로그램을 통한 악성 행위가 많이 발생했던 달이기도 했습니다. 이번 달에는 12월에 발생했던 확장 프로그램 및 애드온 프로그램을 통한 악성 행위 사례에 대해 몇 가지 소개해 드리겠습니다.

먼저 유명한 해외 A,B 사들의 보안 프로그램들과 함께 설치되었던 브라우저 확장 프로그램이 크롬과 파이어폭스 사용자의 브라우징 히스토리를 동의없이 수집했는데, 이 부분은 애초에 사용자가 악성 및 피싱 웹사이트를 방문할 경우 경고하는 역할을 하기 위해 설계된 확장 프로그램이었지만 사용자의 브라우징 습관에 대한 대량의 데이터를 사용자 동의없이 회사 서버로 보내고 있다는 부분이 확인되어 해외에서 크게 논란이 되었습니다.

이 뿐만 아니라, Elementor 및 Beaver 라는 워드프레스 애드온 프로그램의 인증 우회 취약점을 악용하여 패스워드 없이 원격으로 사이트의 관리 권한에 접근하여 워드프레스 기반의 사이트를 해킹할 수 있게 되는 문제가 있었는데 위의 두 애드온 프로그램이 설치된 사이트가 수십만 곳이라 피해를 입은 범위가 꽤 넓을 것으로 예상되며 지금 역시도 피해를 입고 있을 것으로 예상이 되고 있습니다.

또한 크롬 확장 프로그램이 웹페이지에 가상화페 지갑 및 가상 화폐 포털의 패스워드와 개인키를 훔치는 자바 스크립트 코드를 인젝션한 것이 확인되기도 했습니다.

이렇듯 편리한 웹서핑과 사이트운동을 돕는 확장프로그램과 애드온 프로그램이 심각한 보안위험을 초래할 수 있다는 점을 반드시 명심하시고, 사용하지 않는 확장/애드온 프로그램은 반드시 제거하고 되도록 확장/애드온 프로그램 사용은 지양하시되, 꼭 사용해야 하는 확장/애드온 프로그램이라면 최신버전 업데이트 및 보안취약점 점검을 진행하시는 것이 안전함을 기억하시기 바랍니다.

또한, 이중 인증, DB 분리 등의 추가 보안조치 작업을 고려해보시는 것도 필요해 보입니다.

안전하고 편안한 새해 되시기 바랍니다. 올 한해도 열심히 뛰는 이스트시큐리티가 되겠습니다.
감사합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2019 년 12 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 11 월에 각각 1 위를 차지했었던 Misc.HackTool.AutoKMS 이 12 월에도 동일하게 1 위를 차지했으며, 11 월에 각각 2 위와 3 위를 차지했던 Hosts.media.opencandy.com 과 Trojan.Agent.gen 이 12 월에도 동일한 순위를 기록했다. 전반적으로 큰 순위 변동이나 특이사항이 없었던 12 월이었다.

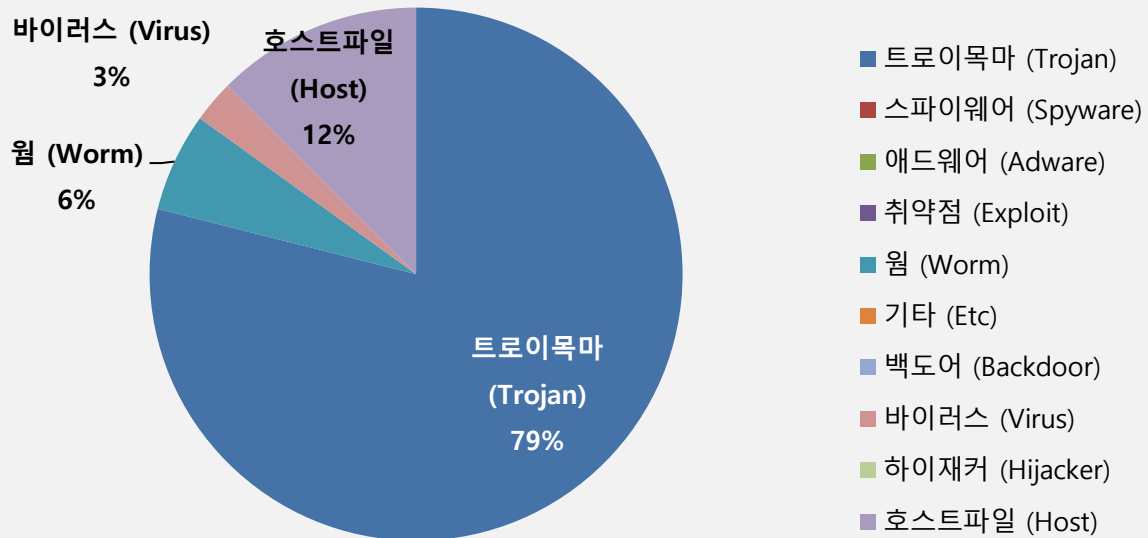
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.HackTool.AutoKMS	Trojan	629,619
2	-	Hosts.media.opencandy.com	Host	549,777
3	-	Trojan.Agent.gen	Trojan	478,360
4	↑1	Trojan.ShadowBrokers.A	Trojan	419,176
5	↑2	Heur.BZC.YAX.Pantera.54.029FDD82	Trojan	352,034
6	-	Gen:Variant.Razy.553929	Trojan	336,877
7	↑1	Misc.HackTool.KMSActivator	Trojan	322,230
8	↑1	Trojan.HTML.Ramnit.A	Trojan	310,249
9	↑1	Misc.Keygen	Trojan	191,529
10	↑2	Misc.Riskware.TunMirror	Trojan	161,594
11	↑3	Worm.ACAD.Bursted	Worm	157,546
12	New	Gen:Variant.Mikey.101080	Trojan	136,689
13	↓2	Misc.Riskware.BitCoinMiner	Trojan	131,595
14	New	Win32.Sality.3	Virus	112,249
15	New	Worm.ACAD.Kenilfe	Worm	106,099

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019년 12 월 01 일 ~ 2019년 12 월 31 일

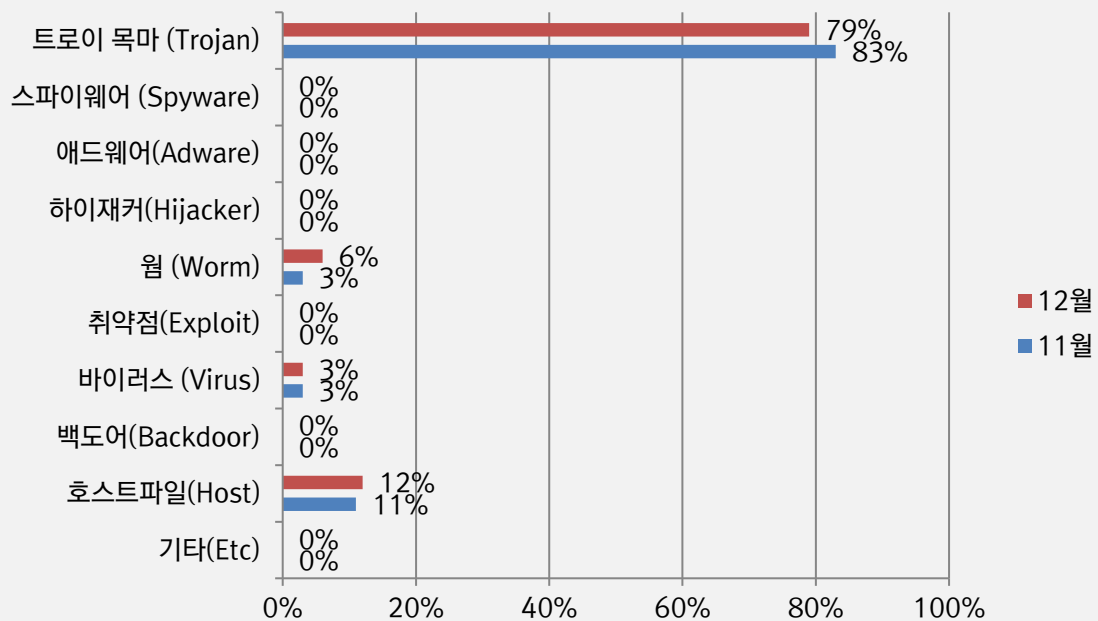
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 79%를 차지했으며 호스트파일(Host) 유형이 12%로 그 뒤를 이었다. 전반적으로 11 월에 비해 전체 감염건수는 7.1% 가량 감소했다.



카테고리별 악성코드 비율 전월 비교

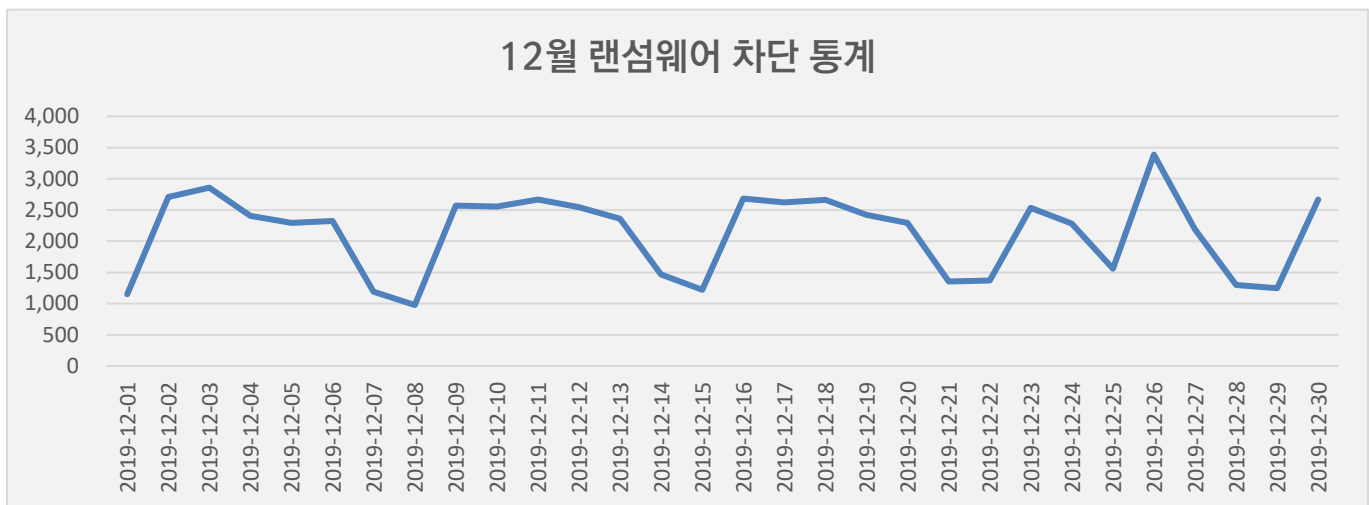
12 월에는 11 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 소폭 감소했으며, 웜(Worm) 유형 악성코드 비율이 소폭 증가했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

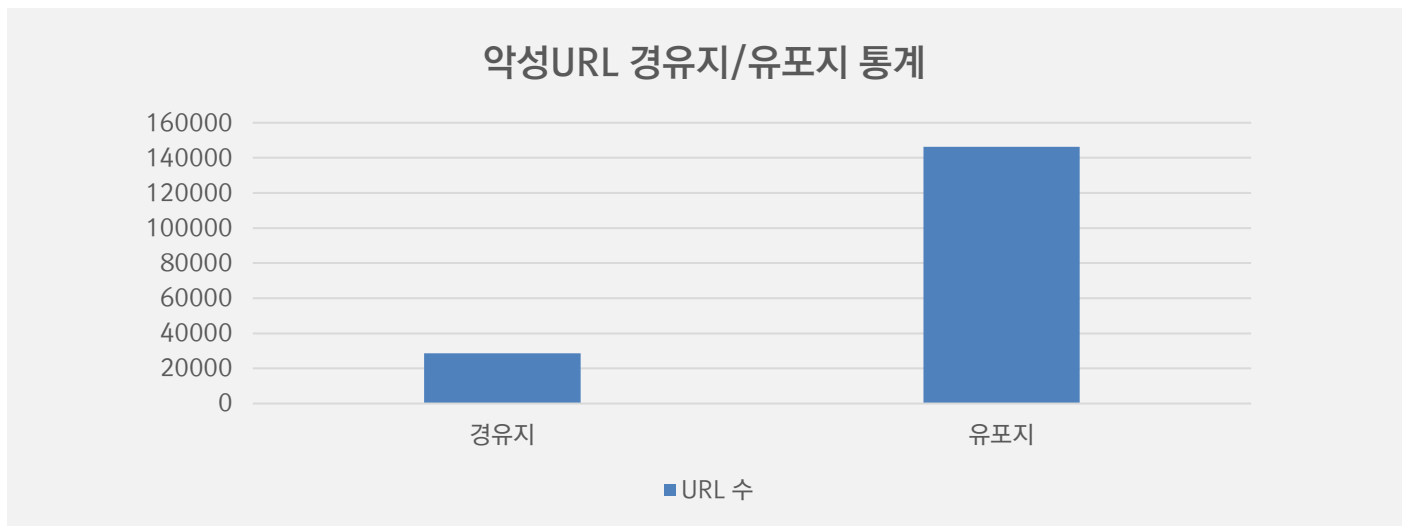
12 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB에 의한 시그니처 탐지횟수는 통계에 포함되지 않는다. 12월 1일부터 12월 31일까지 총 65,893건의 랜섬웨어 공격시도가 차단되었다. 11월에 비해 랜섬웨어 공격건수는 약 2% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 12월 한달간 총 174,822건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 11월 한달간 확인되었던 143,391건의 악성코드 경유지/유포지 URL 수에 비해 21% 정도 증가한 수치다. 경유지 수치는 크게 감소한 반면, 유포지 수치는 대규모로 증가한 부분이 인상적이다. 악성코드 경유지/유포지 URL의 경우 항상 고정적인 URL만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주기 바란다.



02

전문가 보안 기고

1. Apple iPhone 분실 관련 스미싱 메시지 주의!
2. 크리덴셜 스테핑(Credential Stuffing) 공격으로 인한 클라우드 보안 주의!

1. Apple iPhone 분실 관련 스미싱 메시지 주의!

최근 Apple iPhone 분실 관련 메시지가 iMessage 를 이용하여 유포되고 있는 정황이 포착되었습니다. 수신된 iMessage 내용은 아래와 같습니다.



[그림 1] iMessage 로 발송된 스미싱 메시지(출처: 네이버 지식인)

※ 스미싱 상세내용

Apple 고객센터

고객님 안녕하세요. 고객님의께서 분실하신 아이폰 찾았습니다. 아래의 주소 <https://www.apple.com-sr.kr> 연결하여 상세한 위치를 확인하고 기기를 활성화하십시오. 고객님의 아이폰 찾기에 협조해드리겠습니다.

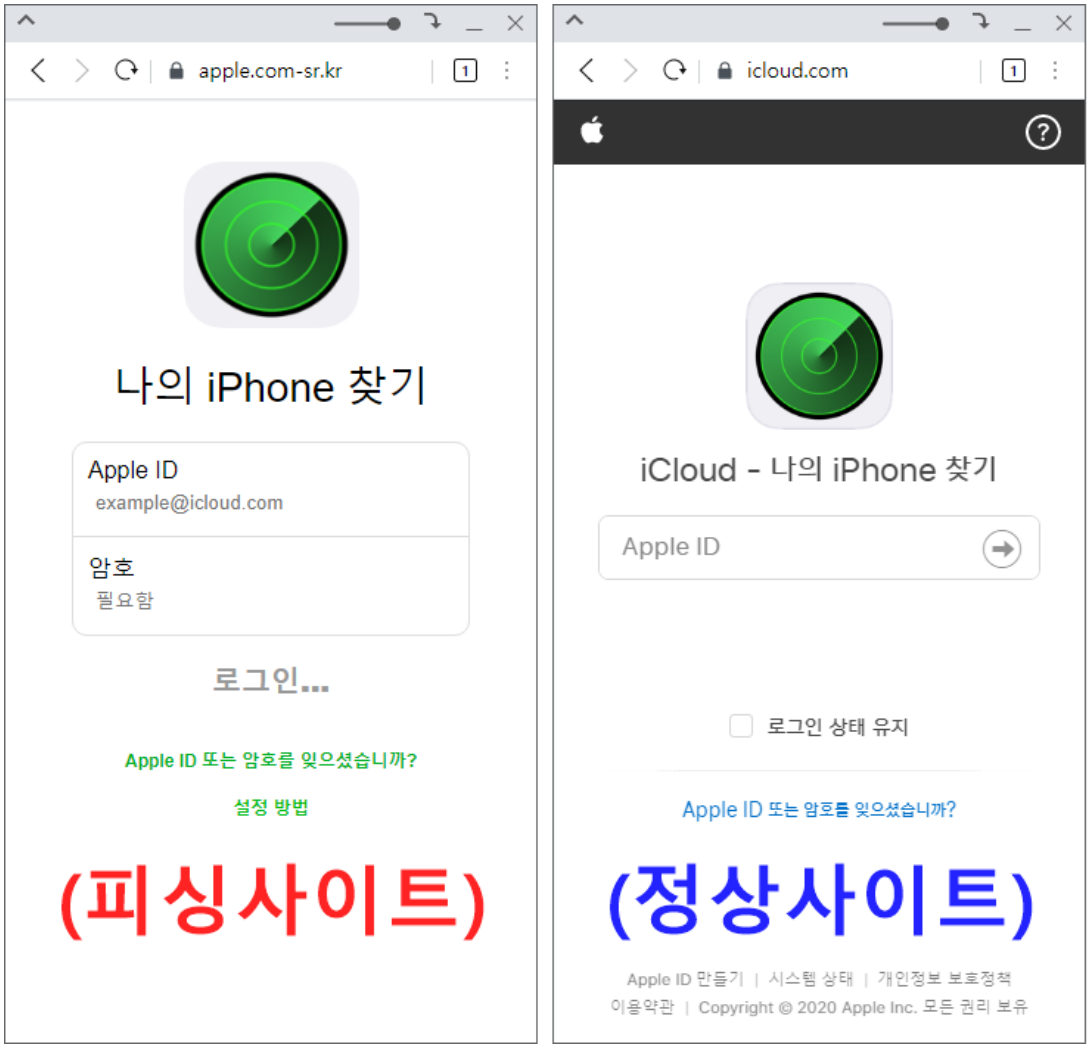
Apple 지원팀

Apple 고객센터

고객님 안녕하세요. 고객님의께서 분실하신 iPhone XS Max 를 찾았습니다. 고객님의께서 <https://www.apple.com-sr.kr> 에 등록하여 상세한 정보를 확인하고 기기를 활성화하십시오. 그리고 고객님의 iPhone 찾기에 협조해 드리겠습니다.

Apple 지원팀

스미싱 메시지에 포함된 링크를 클릭할 경우 사용자의 Apple 계정을 탈취하기 위한 피싱 사이트로 이동됩니다. 피싱 사이트에는 “나의 iPhone 찾기”라는 문구와 함께 분실된 기기를 찾는다면 사용자의 Apple 계정을 요구합니다.

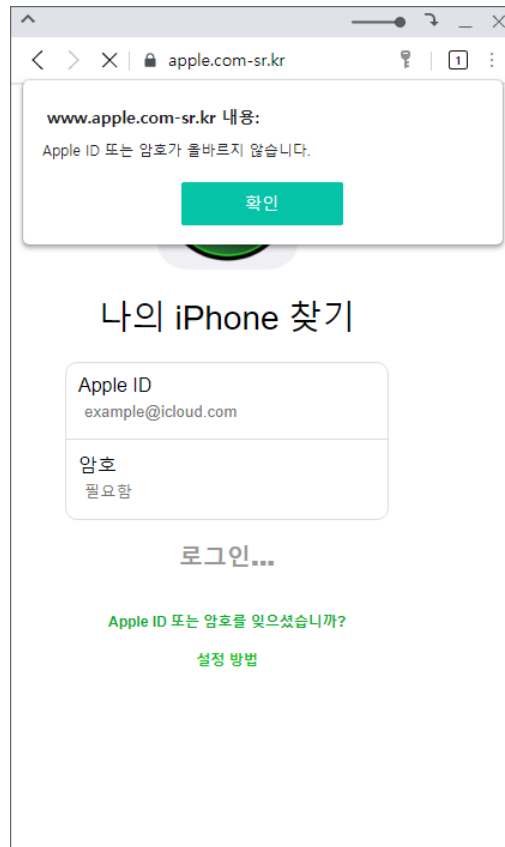


[그림 2] Apple ID를 탈취하기 위한 피싱 사이트와 정상 사이트 비교 화면

02 전문가 기고

사용자가 실제 Apple 로그인 계정과 패스워드를 입력할 경우, 개인정보 수집 사이트로 계정 정보가 전송되며, 개인정보가 전달된 후에는 미리 설정된 스크립트가 동작하면서 사용자에게 로그인 실패 경고 창을 팝업하고 다수의 입력을 요청합니다.

```
<script language=JavaScript>window.alert('Apple ID 또는 암호가 올바르지 않습니다.');
```



[그림 3] 수집된 개인정보 내용

전송된 개인정보 수집 도메인 정보 및 내용을 상세히 살펴보면 다음과 같습니다.

Body	
Name	Value
q	hongkildong@icloud.com
w	1q2w3e4r
submit	로그인...
act	ok

[그림 4] 수집된 개인정보 내용

02 전문가 기고

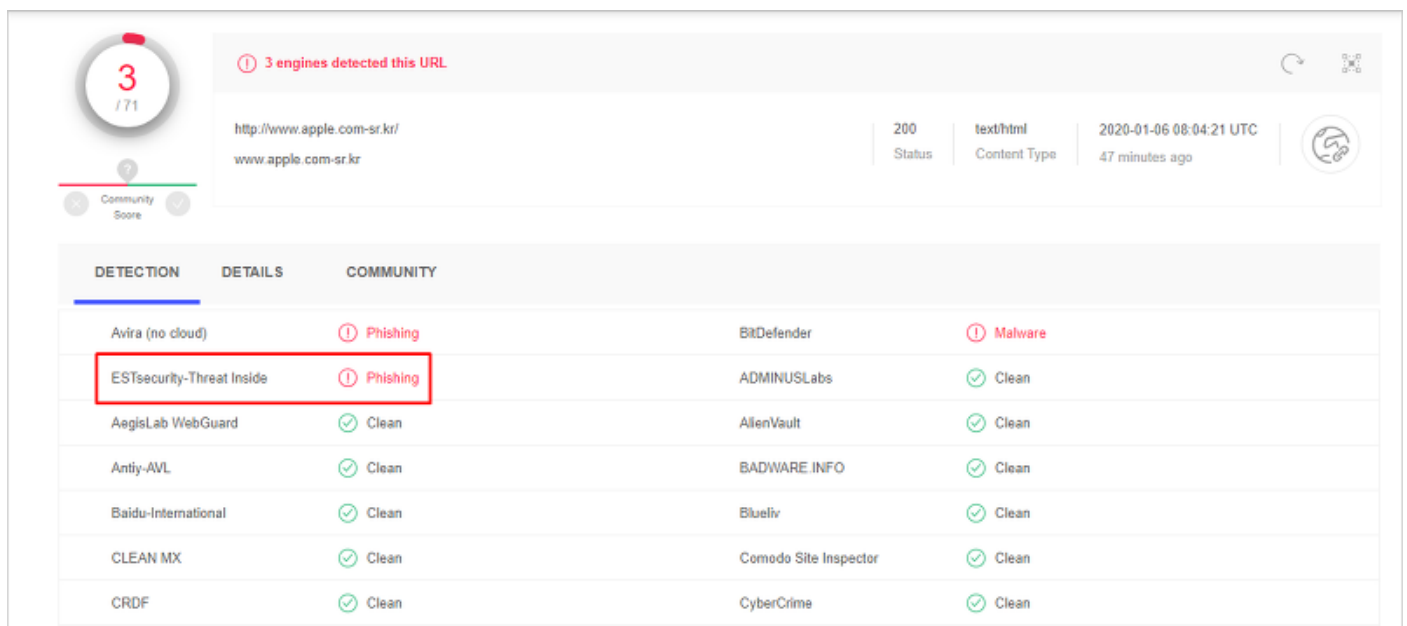
※ 개인정보 수집 사이트 상세 정보

개인정보 파싱 사이트 : [https://www.apple.com-sr\[.\]kr](https://www.apple.com-sr[.]kr)

개인정보 전달 사이트 : [https://www.apple.com-sr.kr/find/wap1\[.\]asp](https://www.apple.com-sr.kr/find/wap1[.]asp)

개인정보 전달 서버 IP : 45.138.209[.]185 (KR)

나날이 정교해지는 스미싱을 대비하기 위해 메시지에 포함되어 있는 출처가 불분명한 링크에 대한 접근을 지양해야 합니다. 현재 이스트시큐리티 ‘쓰렛 인사이드(Threat Inside)’에서는 해당 개인정보 수집 사이트를 아래와 같이 탐지하고 있습니다.



3 / 71

3 engines detected this URL

http://www.apple.com-sr.kr/
www.apple.com-sr.kr

200 Status
text/html Content Type
2020-01-06 08:04:21 UTC
47 minutes ago

DETECTION	DETAILS	COMMUNITY
Avira (no cloud)	① Phishing	BitDefender ① Malware
ESTsecurity-Threat Inside	① Phishing	ADMINUSLabs ✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault ✓ Clean
Antiy-AVL	✓ Clean	BADWARE.INFO ✓ Clean
Baidu-International	✓ Clean	Blueliv ✓ Clean
CLEAN MX	✓ Clean	Comodo Site Inspector ✓ Clean
CRDF	✓ Clean	CyberCrime ✓ Clean

2. 크리덴셜 스테핑(Credential Stuffing) 공격으로 인한 클라우드 보안 주의!

최근 일부 연예인들의 스마트 폰이 해킹당해 문자메시지 등 개인정보가 유출되었다는 이슈가 연일 화제를 낳고 있습니다.

이번 사건은 초기에 스미싱이나 악성앱 감염으로 인한 위협노출 등 다양한 형태가 추정되었지만, 다른 곳에서 유출된 개인정보로 인한 2 차 피해, 즉 크리덴셜 스테핑의 가능성에 무게가 실리고 있습니다.

* 크리덴셜 스테핑(Credential Stuffing)이란?

공격자가 여러 가지의 경로로 수집한 사용자들의 로그인 인증 정보(Credential)를 다른 사이트의 계정 정보에 마구 대입(Stuffing)하는 공격 방식

일반적으로 사용자들은 인터넷에서 자신만 사용하는 고유의 아이디를 갖고 있으며, 편의를 위하여 다양한 사이트에 동일한 로그인 인증정보를 공통으로 사용하는 경우가 있습니다.

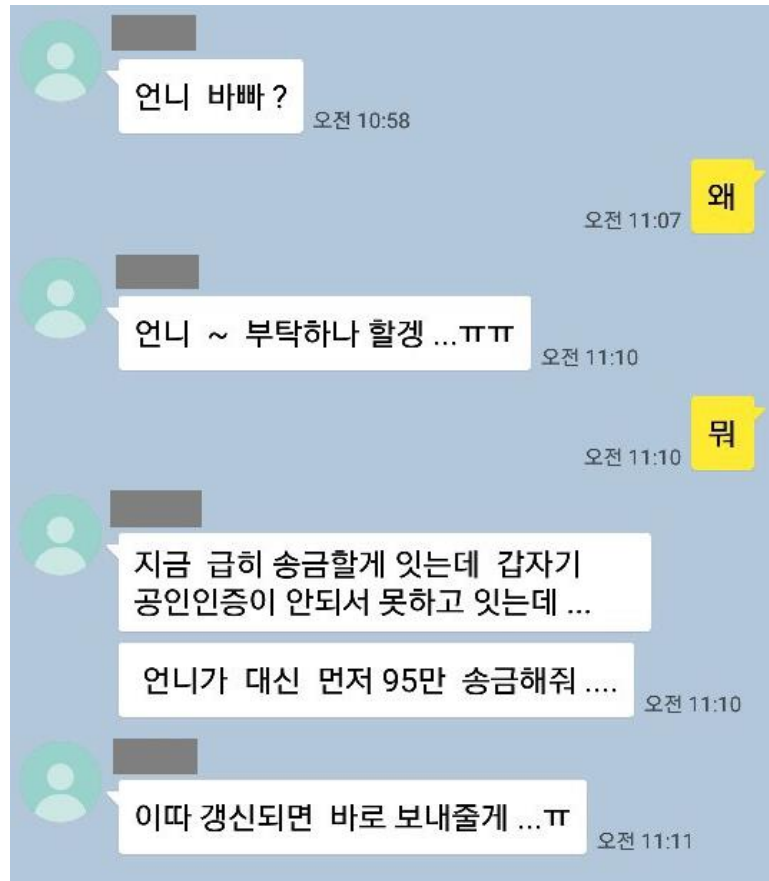
일정 수준 이상의 규모를 가진 인터넷 서비스 기업들은 상당한 수준의 정보보안 체계를 구축하고 있기 때문에 고객들의 정보는 나름 높은 보안 수준으로 안전하게 보호되고 있습니다.

그렇기 때문에 공격자들은 상대적으로 취약한 보안체계를 구축하고 있는 영세한 웹사이트들을 공격 타겟으로 삼는 경우가 많습니다.

만약 이러한 사이트가 해킹을 당해 계정 유출사고가 발생하였다면, 해킹당한 사이트와 동일한 계정 정보(아이디, 비밀번호)를 사용하는 곳들의 개인정보는 잠재적 위협에 노출될 수 있다고 볼 수 있습니다.

하지만 해킹이 발생한다 해도 유출된 로그인 정보주체뿐만 아니라 해킹된 사이트의 정보보호 관리자들도 역시 해킹된 사실을 인지하지 못하는 경우가 많습니다.

몇 년 전부터 현재까지 지속되고 있는 국내 유명 메신저 사칭 사건 역시 크리덴셜 스테핑 공격이라고 볼 수 있습니다.



[그림 1] 유명 메신저사칭사기사례

〈이미지 출처: 네이버〉

누군가 자신을 사칭해 메신저에서 지인들, 혹은 가족들에게 금전을 요구하는 경우입니다.

실제 내 휴대폰은 해킹당하지 않았는데, 어떻게 내 지인들 및 가족들의 정보를 과연 어떻게 알았을까?라는 의구심이 들수도 있지만, 이것 역시 크리덴셜 스테핑 공격의 일환입니다.

즉, 어딘가에서 사용자의 로그인 계정 정보가 유출되었고, 만약 그 사용자가 자신의 휴대폰과 동기화된 클라우드 주소록에서 유출된 정보와 동일한 로그인 계정 정보를 사용하고 있다면, 해커들은 손쉽게 사용자 휴대폰 주소록에 있는 정보들을 획득할 수 있는 것입니다.

이름 ↑		전화번호
<input type="checkbox"/> ☆ 강		02-57
<input type="checkbox"/> ☆ 강		010-6 9
<input type="checkbox"/> ☆ 강		010-4 6
<input type="checkbox"/> ☆ 고		010-9 8
<input type="checkbox"/> ☆ 구		010-9 8
<input type="checkbox"/> ☆ 구		010-2 1
<input type="checkbox"/> ☆ 김		010-2 2
<input type="checkbox"/> ☆ 김		010-7 3
<input type="checkbox"/> ☆ 김		010-5 1
<input type="checkbox"/> ☆ 김		019-9 9
<input type="checkbox"/> ☆ 김		07040
<input type="checkbox"/> ☆ 김		010-6 4
<input type="checkbox"/> ☆ 김		010-5 6
<input type="checkbox"/> ☆ 김		010-8 0

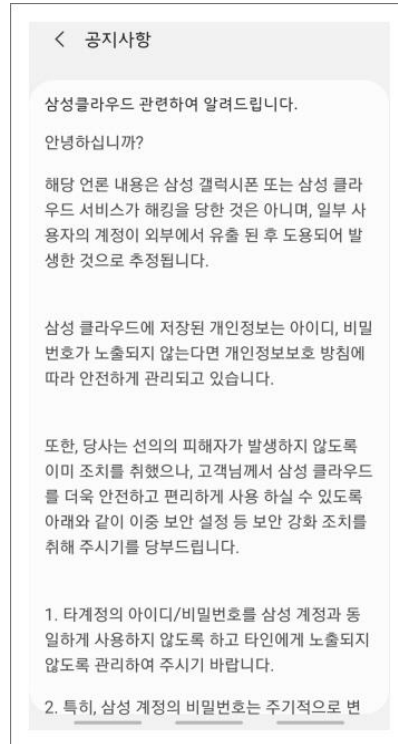
[그림 2] 클라우드 주소록에 백업되어 있는 주소목록

실제 클라우드 주소록 서비스를 확인해 보면 내 휴대폰에 저장되어있는 정보들과 동일한 정보들이 백업되어있는 것을 볼 수 있습니다.

이렇게 유출된 개인정보로 인한 2 차 피해를 방지하려면 사이트마다 다른 비밀번호를 사용해야 합니다. 하지만 비밀번호를 모두 다르게 설정하기가 힘들다면, 최소한 2 단계 인증을 설정해 놓아야 합니다.

2 단계 인증이란, 계정 정보 이외에 또 다른 정보(예를 들어 SMS 로 전송되는 인증코드 등)를 입력해야만 본인 인증을 하는 방식입니다. 만약 계정 정보가 유출되었다고 하더라도 추가적인 정보를 확인할 수 없기 때문에 계정에 로그인할 수 없게 됩니다.

이번 사건과 관련하여 삼성도 역시 안전한 계정 사용을 위해 2 단계 인증을 설정하라고 권고하고 있습니다.



[그림 3] 삼성클라우드 공지사항

이밖에도 대형 사이트들에서는 2 단계 인증 기능을 제공하고 있기 때문에 유출된 개인정보로 인한 2 차 피해를 예방하기 위해서는 반드시 자주 사용하는 사이트의 2 단계 인증 기능을 활성화해놓으시기 바랍니다.

※ 2 단계 인증 설정 방법

▶ 삼성계정

휴대폰 설정 > 계정 > 삼성 계정 > 비밀번호 및 보안 > 2 단계 인증 메뉴 활성화

▶ Apple ID

휴대폰 설정 > 사용자 이름 > 암호 및 보안 > 이중인증 켜기 > 계속

▶ 네이버

계정 로그인 > 내정보 > 보안설정 > 비밀번호 (2 단계 인증) > 설정

▶ 다음카카오

계정 로그인 > 내정보 > 2 단계 인증 > 설정

▶ 구글

계정 로그인 > google 계정관리 > 보안 > 2 단계 인증 > 설정

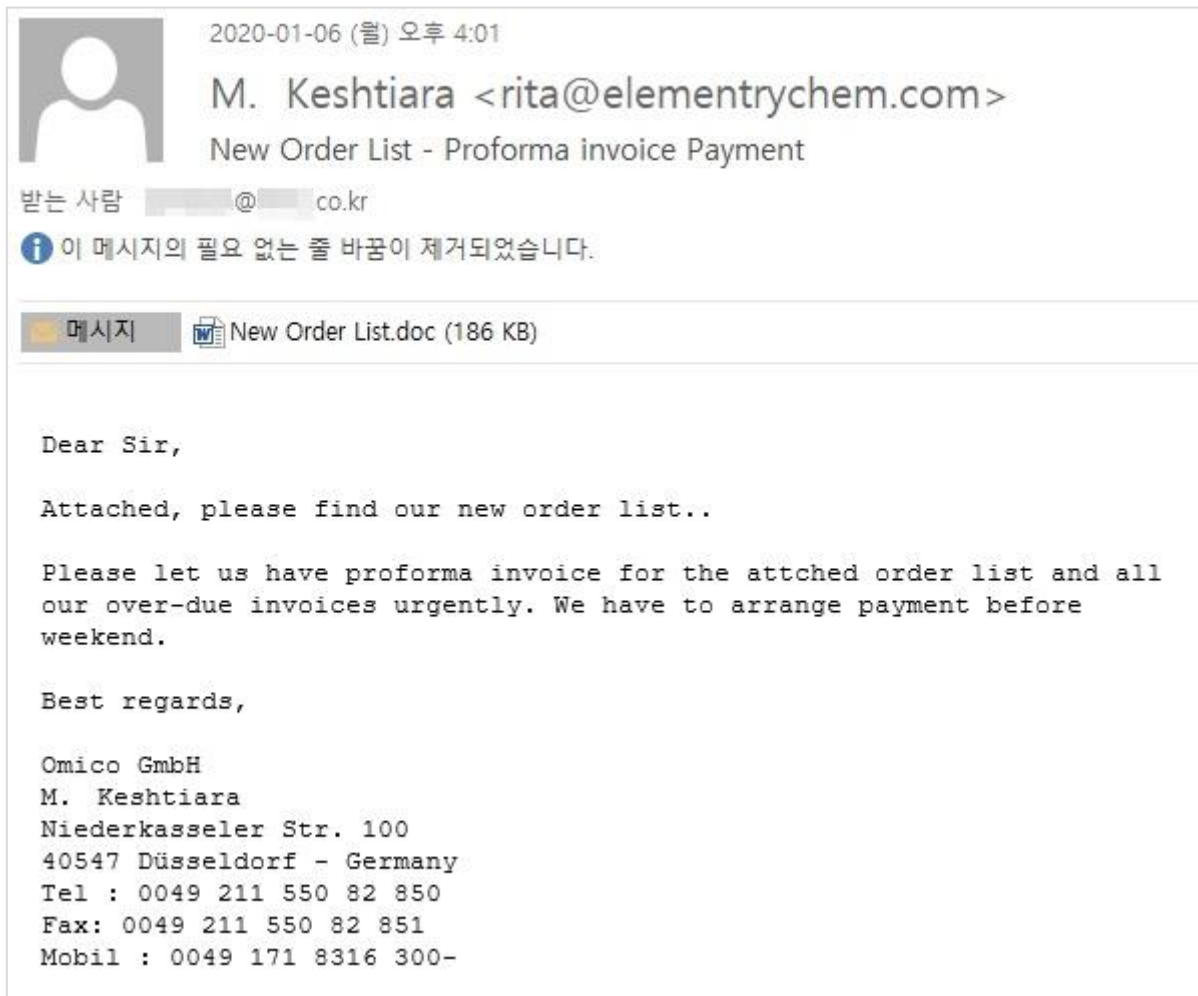
03

악성코드 분석 보고

[Trojan.PSW.AveMaria]

악성코드 분석 보고서

최근 국내 기업에 주문 리스트를 확인해달라는 내용의 메일로 'Trojan.PSW.AveMaria'(이하 'AveMaria') 악성코드가 유포되고 있다. 'AveMaria'는 메일에 첨부된 'New Order List.doc' 악성 문서 파일에서 드롭되어 실행된다.



[그림] 주문 리스트 확인 악성 메일

악성 문서 파일에서 실행되는 'AveMaria'는 명령 제어 기능을 수행한다. C&C 에서 공격자 명령에 따라 감염 PC 정보 수집, 웹 브라우저 및 전자 메일 프로그램에 저장된 계정 정보 탈취, 키로깅 등의 다양한 악성 기능이 수행될 수 있어서 사용자들의 주의가 필요하다.

현재 알약에서는 해당 악성 코드를 'Trojan.PSW.AveMaria' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

[Trojan.Android.InfoStealer]

악성코드 분석 보고서

해당 악성 앱은 안드로이드의 웹 뷰 기능을 통해서 특정 성인 사이트를 로드한다.

기기의 전화번호 정보를 수집하며 주소록, 통화목록, 문자 관련 개인 정보를 xml 파일로 저장하고 압축 후 C&C 서버로 탈취한다.

Destination	Protocol	Length	Info
45.77.28.178	TCP	74	51234 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=146
45.77.28.178	TCP	74	[TCP Retransmission] 51234 → 80 [SYN] Seq=0 Wi
45.77.28.178	TCP	74	[TCP Retransmission] 51234 → 80 [SYN] Seq=0 Wi
45.77.28.178	TCP	74	[TCP Retransmission] 51234 → 80 [SYN] Seq=0 Wi
45.77.28.178	TCP	74	[TCP Retransmission] 51234 → 80 [SYN] Seq=0 Wi
45.77.28.178	TCP	74	[TCP Retransmission] 51234 → 80 [SYN] Seq=0 Wi

[그림] C&C로 탈취되는 정보

해당 악성 앱은 성인 앱으로 속이며 개인 및 기기와 관련된 다양한 정보를 탈취한다.

따라서 악성 앱으로부터 피해를 최소화하기 위해서는 백신 앱을 통한 주기적인 검사가 중요하다. 출처가 불명확한 URL 과 파일은 실행하지 않는 것이 기본이고 공식 마켓인 구글 플레이스토어를 통해서 확보한 앱이라도 백신 앱을 추가 설치하여 주기적으로 업데이트하고 검사해야 한다.

현재 알약M에서는 해당 악성 앱을 'Trojan.Android.InfoStealer' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

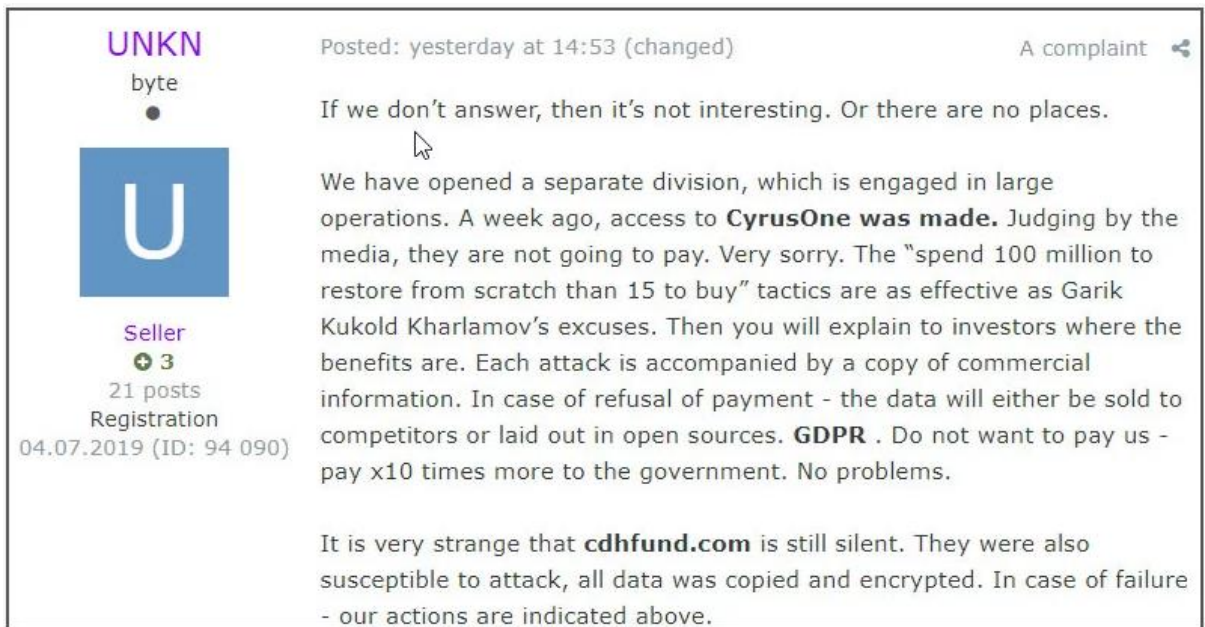
04

글로벌 보안 동향

REvil 랜섬웨어, 피해자가 돈을 지불하지 않으면 데이터를 공개하겠다고 협박해

Another Ransomware Will Now Publish Victims' Data If Not Paid

Sodinokibi 라고도 알려진 REvil 랜섬웨어의 운영자들이 피해자가 랜섬머니를 지불하지 않을 경우 지불하도록 하기 위해 훔친 파일과 데이터를 활용하겠다고 밝혔다. 이들의 새로운 전략은 피해자가 돈을 지불하지 않을 경우 데이터를 공개하는 것이다. Maze 랜섬웨어 또한 과거 비슷한 행보를 보였다. 보안 연구원인 Damian 이 공개한 러시아 악성코드 및 해커 포럼의 포스팅에 따르면, REvil 랜섬웨어의 공식적인 대변인인 UNKN 은 대규모 작업을 위한 새로운 부서를 만들었으며, 이들은 CyrusOne 데이터 센터에서 발생한 공격이 자신들의 소행이라 밝혔다. UNKN 은 이 회사의 네트워크를 암호화하기 전 회사의 파일을 훔쳤다고 주장했다. REvil 은 랜섬머니를 지불하지 않을 경우, 훔친 데이터를 공개하거나 경쟁사에게 판매하겠다고 했으며, 이는 랜섬머니를 지불하는 것보다 훨씬 더 많은 비용을 지불하게 될 것이라고도 덧붙였다.



랜섬웨어 공격, 이제는 데이터 유출 사건으로 간주해야

지난 몇 년 동안 랜섬웨어 개발자와 제휴 파트너들은 피해자들에게 몸값을 지불하지 않을 경우 훔친 데이터를 공개할 것이라 협박해왔다. 랜섬웨어 공격자들이 피해자의 데이터를 훔쳐보고 데이터가 암호화되기 전에 수집한다는 사실은 공공연한 비밀이었으나, 아직까지 실제로 데이터를 유출한 사례는 없었다. 하지만 지난 11 월 말 Maze 랜섬웨어가 Allied Universal 을 협박해 랜섬머니를 지불하지 않으면 파일을 공개하겠다고 위협한 사례가 있었다. 이들은 랜섬머니를 받아내지 못했으며 데이터 약 700MB 가 해킹 포럼에 공개되었다.

Allied Universal의 데이터 공개

일부 공격자들은 랜섬웨어 피해를 입은 회사에 그들의 파일을 읽은 후 회사의 내부 기밀을 알게 됐다고 알렸다. 이 경우 명백히 데이터 유출 사건으로 간주되어야 하지만, 많은 랜섬웨어 피해 업체들은 그저 들키지 않기만을 바라며 사건을 그대로 덮어버렸다. 이제 랜섬웨어 공격자들이 피해자의 데이터를 공개하고 있기 때문에, 회사는 랜섬웨어 감염 발생 시 데이터 유출 사건으로 간주해야 할 것이다. 이 경우 직원의 의료 기록, 개인 정보, 해고 통지서, 급여 등과 같은 정보가 공개될 가능성이 있기 때문이다. 또한 제삼자의 정보가 도난당했을 경우 추가로 정보를 공개해야 한다. 이러한 랜섬웨어의 전략 변경 이후 기업들이 랜섬웨어 공격을 데이터 유출로 간주하도록 압력을 가할 수 있을지 여부는 불투명하다. 하지만 더 많은 랜섬웨어 개발자들이 훔친 문서를 공개할수록 소송에 휘말릴 가능성 및 대중의 관심은 높아질 것이다.

[출처] <https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/>

안티바이러스 우회를 위해 Windows 를 안전 모드로 재부팅하는 Snatch 랜섬웨어 발견

Snatch Ransomware Reboots Windows in Safe Mode to Bypass Antivirus

사이버 보안 연구원들이 안티바이러스 탐지를 피하기 위해 감염된 Windows 컴퓨터를 안전모드로 재부팅 후 피해자의 파일을 암호화하는 Snatch 랜섬웨어의 새로운 변종을 발견했다. 다른 기존의 악성코드와는 달리 새로운 Snatch 랜섬웨어는 안전모드에서 실행된다. Windows OS 는 진단 모드에서 안티바이러스 소프트웨어를 포함한 대부분의 타사 시작 프로그램을 로드하지 않고 최소한의 드라이버와 서비스만을 로드하기 때문이다. Snatch 는 2018 년 여름부터 활동해 왔지만, SophosLabs 의 연구원들은 최근 다양한 피해자들을 대상으로 이루어진 최근 사이버 공격에서만 이 안전 모드 재부팅 기능을 발견했다고 밝혔다.


Snatch 랜섬웨어는 Windows 레지스트리를 이용하여 자기 자신을 안전 모드 부팅 중 실행되는 서비스인 ‘SuperBackupMan’ 으로 설정한다. 컴퓨터가 재부팅되면 안전 모드가 활성화되며, 이 악성코드는 Windows 컴포넌트인 net.exe 를 사용하여 SuperBackupMan 서비스를 중단시킨 후 Windows 컴포넌트인 vssadmin.exe 를 사용하여 컴퓨터 내 모든 볼륨 새도 복사본을 삭제하여 랜섬웨어로 암호화된 파일을 복구할 수 없도록 한다. Snatch 는 랜섬웨어 기능뿐 아니라 데이터 스틸러의 기능 또한 포함하고 있어 보다 위험한 것으로 드러났다. Snatch 는 정교한 데이터 스틸링 모듈을 포함하고 있어 공격자가 타깃 조직으로부터 방대한 정보를 훔칠 수 있게 된다.

영상: <https://vimeo.com/378363798#at=1>

Snatch 는 크로스 플랫폼 앱 개발용으로 알려진 프로그래밍 언어인 Go 언어로 작성되었지만, 이 랜섬웨어는 Windows 플랫폼에서만 동작하도록 설계되었다. 한 보안 전문가는 Snatch 는 Windows 7~10, 32 비트 및 64 비트 버전에서 모두 실행될 수 있으며, 발견한 샘플은 콘텐츠를 난독화하기 위해 오픈 소스 패커인 UPX 로 패키징되어 있었다고 밝혔다. 이 외에도, Snatch 랜섬웨어 운영자는 대규모 조직에 랜섬웨어를 배포하기 위해 악용이 가능한 크리덴셜과 백도어를 보유한 다른 사이버 범죄자들에게 파트너십을 제안하기도 한다. 아래 스크린샷과 같이 언더그라운드 포럼에서는 “기업 네트워크 및 상점, 기타 회사에 RDP \ VNC \ TeamViewer \ WebShell \ SQL 인젝션 접근이 가능한 제휴 파트너를 찾고 있다” 라는 글이 포스팅되기도 했다.

● BulletToothTony

★



Пользователь
Сообщений: 7
Репутация: 21

Опубликовано 12 августа

Набираем адвертов с доступами RDP\VNC\TeamViewer\WebShell\SQL inj к копоративным сетям, шопам и прочим компаниям

За подробностями в РМ. В сообщении кратко опишите интересующие вас вопросы, тип материала и другие детали. Это повысит вероятность быстрого ответа. Давайте будем уважать свое и наше время

Спасибо

р.с. Набор на обучение завершен, группа сформирована и занятия уже идут. Открытие набора в новые группы будет анонсировано в первом топике. Просьба не писать в РМ касательно обучения

공격자들은 브루트포싱 공격을 실행하거나 훔친 크리덴셜을 이용하여 기업의 내부 네트워크에 접근한 후 정식 시스템 관리자 및 침투 테스트 툴을 통해 탐지되지 않은 채 해당 네트워크에 연결된 다른 기기를 해킹한다. 범죄자들은 Process Hacker, IObit Uninstaller, PowerTool, PsExec 등 타깃 네트워크 내 기기에 설치된 다양한 정식 툴을 악용했으며, 일반적으로 안티바이러스 제품을 비활성화하기 위한 목적으로 이러한 툴을 사용했다. 랜섬웨어 전문 협상 업체인 Coveware는 Sophos 측에 2019년 7월~10월 사이에 클라이언트 12곳이 Snatch의 공격자들과 협상을 진행했으며, 그들이 요구한 랜섬머니는 비트코인으로 약 \$2,000 ~ \$35,000 사이였다고 밝혔다. 이러한 랜섬웨어의 공격으로부터 조직을 보호하기 위해서는 중요 서비스와 보안 포트를 인터넷에 연결하는 것을 지양하고, 다중 인증을 통한 강력한 패스워드로 보안을 강화해야 한다.

[출처] <https://thehackemews.com/2019/12/snatch-ransomware-safe-mode.html>

<https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/>

Citrix NetScaler 에서 회사 8 만 곳에 영향을 미치는 치명적인 버그 발견 돼

This critical Citrix NetScaler bug could affect 80,000 companies

Citrix 가 최소 8 만 곳의 조직에 영향을 미치는 Citrix ADC(Application Delivery Controller)의 심각도 높은 버그를 공개했다. 현재 이 취약점에 대한 패치는 공개되지 않은 상황이다.

Citrix 에 따르면 공격자가 이 버그를 악용할 경우 적절한 인증 과정을 거치지 않아도 임의로 코드를 실행할 수 있는 것으로 나타났다.

취약한 제품은 NetScaler ADC, Citrix Gateway 또는 NetScaler Gateway 다. 이 버그는 CVE-2019-19781 로 등록되었다.

지금 이 크리스마스 연휴임을 감안할 때, Citrix 의 취약점 공개 시기는 꽤 위험하다고 볼 수 있다. 미국, 영국, 호주 전역의 기업 네트워크에서 폭넓게 사용되는 Citrix 장비를 관리하는 IT 관리자들은 더욱 주의를 기울여야 하겠다.

안타깝게도 현재까지 패치가 발행되지 않은 상황이며, 대신 Citrix 는 패치가 발표되기 전까지 적용할 수 있는 임시 완화법을 공개했다.

“취약한 제품을 사용할 경우 즉시 완화법을 적용할 것을 강력히 권고한다. 이후 수정된 어플라이언스 펌웨어 버전이 출시 되면 모든 취약한 어플라이언스를 업그레이드 해야할 것이다.”

Citrix 는 또한 관리자들에게 새로운 펌웨어가 준비될 경우 알림을 받을 수 있도록 [알림 게시판](#)을 구독할 것을 권장했다. Citrix 의 완화법은 [여기](#)에서 확인할 수 있다.

이 버그는 영국 보안 회사 Positive Technologies 의 연구원인 Mikhail Klyuchnikov 가 제보하였으며 월요일 버그 리포트를 공개하였다.

Klyuchnikov 는 해당 버그가 158 개국의 8 만 회사에 영향을 미치며, 원격 공격자가 악용할 경우 내부 네트워크를 단 1 분 이내에 해킹할 수 있을 것이라 밝혔다.

“공격자가 이 취약점을 악용할 경우 인터넷에서 회사의 로컬 네트워크로 직접 접근할 수 있는 권한을 얻게 된다. 이 공격을 실행하기 위해서는 어떠한 계정도 필요하지 않으며, 따라서 외부 공격자 누구나 이 공격을 실행할 수 있다.”

Citrix 는 이 버그의 심각도에 대해 점수를 매기지는 않았지만, Positive Technologies 는 10 점 만점에 10 점일 것이라 확신했다.

“이 취약점은 해당 제품의 모든 지원되는 버전의 제품 및 플랫폼에 영향을 미친다. 취약한 버전은 Citrix ADC & Citrix Gateway 13.0, Citrix ADC & NetScaler Gateway 12.1, Citrix ADC & NetScaler Gateway 12.0, Citrix ADC & NetScaler Gateway 11.1, Citrix NetScaler ADC & NetScaler Gateway 10.5 다.

[출처] <https://www.zdnet.com/article/this-critical-citrix-netscaler-bug-could-affect-80000-companies/>

<https://support.citrix.com/article/CTX267027>

<https://support.citrix.com/article/CTX267679>



(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

www.estsecurity.com