이스트시큐리티

보안 동향 보고서

No.128 2020.05

No.128 2020.05

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

2020 년 4 월에도 3 월과 마찬가지 코로나 19 바이러스가 글로벌한 이슈로 전세계적으로 가장 큰 관심을 모으는 이슈로 자리잡으면서 사이버 공격도 코로나 19 키워드를 굉장히 활발하게 활용하고 있는 추세를 보이고 있습니다. 비트코인 시세가 다시 급등하면서 복호화 비용으로 비트코인을 요구하는 랜섬웨어 공격 역시 꾸준히 발생하고 있습니다.

4 월 한달간 코로나 19 바이러스 키워드를 활용한 공격은 다양하게 발생했고, 3 월까지 선보였던 기존 키워드(코로나 19 바이러스 감염현황, 예방법, 치료방법)보다 한단계 더 발전한 마스크, 긴급재난자금 상품권, CDC 로부터의 작업장 폐쇄명령, 코로나 19 바이러스 확산방지 가이드라인 등의 디테일한 키워드를 활용하기 시작한 부분이 주목할 만한 부분이라고 판단됩니다.

특히 4 월에는 한글로 작성된 코로나바이러스 관련 악성메일이 다수 확인되기도 하였으며, 이메일뿐만 아니라 '긴급재난자금' 상품권을 사칭한 스미싱, 저금리 대출 문자메시지로 위장한 카톡 스미싱까지 확인되었습니다.

APT 공격그룹에서도 4 월 한달동안 여러 차례 공격을 시도했는데 앞서 언급했던 코로나 이슈를 활용한 공격은 물론, 4 월에 있었던 21 대 국회의원 선거 문서로 사칭한 스모크스크린 시리즈 APT 공격, 그리고 블록체인 소프트웨어 개발 계약, 한미관계/외교안보 문서, 항공우주기업 채용관련 문서, 성착취물 유포 사건 출석 통지서 등을 소재로 다양한 공격을 시도했습니다.

이외에도 애플 사용자나 모바일 중고거래 사이트 이용자의 계정정보를 노린 피싱 공격도 몇차례 확인되었습니다.

코로나 19 바이러스 확산 방지를 위해 많은 기업들이 재택근무를 시행하고 있고 원격으로 회사 네트워크에 연결되고 있는 상황을 공격자들은 지속적으로 노릴 것으로 생각됩니다.

특히, 꾸준히 활용하던 전통적인 공격 방식 소재에 사용자들이 관심을 많이 가지는 '코로나 19 바이러스' 관련 키워드를 적절히 섞어서 공격을 많이 시도하고 있는데, 악성 문서 파일을 미끼로 주요 기업과 기관의 임직원들을 노리는 위협 활동에 대비하여 각별히 주의를 기울여야 하는 한편, 의심스러운 메일이나 문자메시지, 카카오톡 메시지를 수신할 경우 지체 없이 사내 보안관련 부서나 ESRC(이스트시큐리티 시큐리티대응센터)에 신고해주시면 초기에 조치하거나 위협을 사전에 방지할 수 있음을 꼭 인지해주시기 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 4 월의 감염 악성코드 Top 15 리스트에서는 지난 2020 년 3 월에 1 위를 차지했던 Hosts.media.opencandy.com 가 4 월에도 동일하게 1 위를 차지했으며, 3 월에 2 위를 차지했던 JS:Trojan.Cryxos.2745 가 이번달에도 역시 2 위를 차지했다. Misc.HackTool.AutoKMS 가 지난달 4 위에서 한 계단 순위가 올라 3 위를 차지했다. Misc.HackTool.AutoKMS 는 불법 SW 의 시리얼 넘버를 추출해주는 악성코드가 포함된 키 추출 프로그램으로, 불법 SW 사용시 주로 노출되는 위협이다.

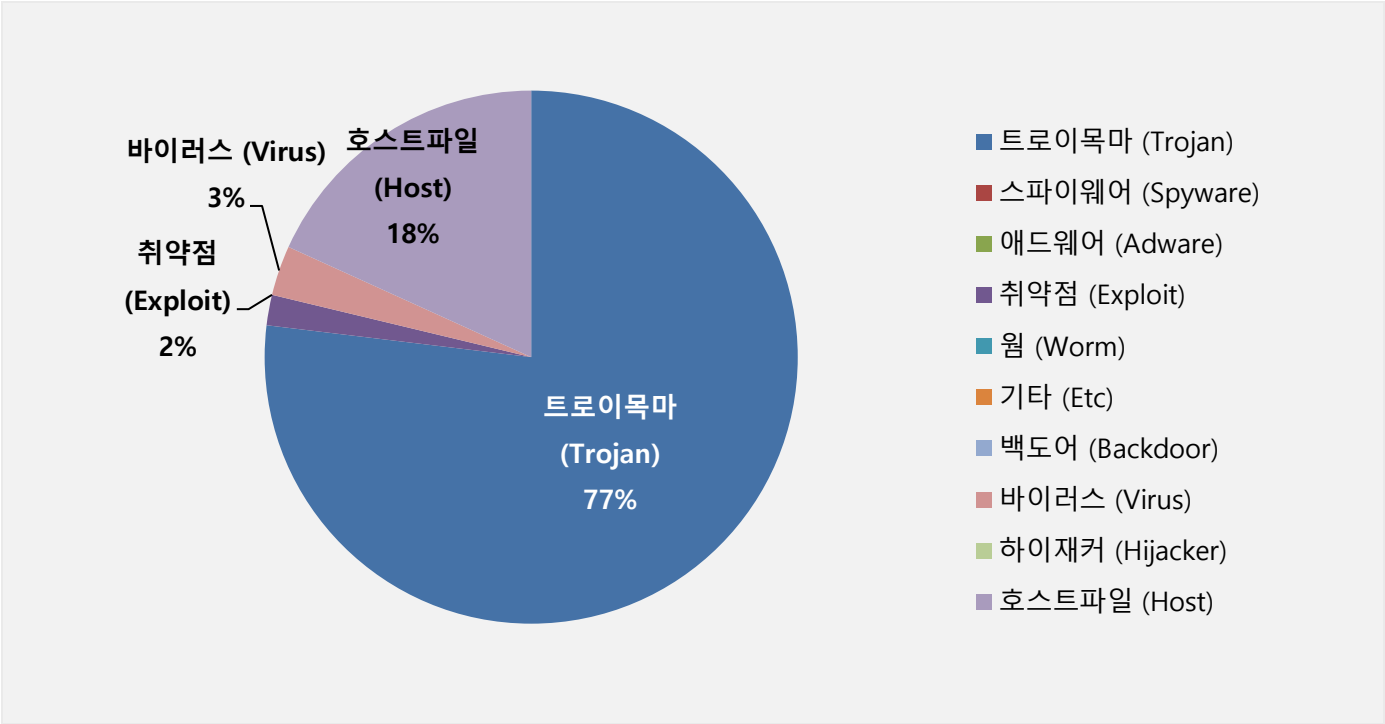
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	968,567
2	-	JS:Trojan.Cryxos.2745	Trojan	933,073
3	↑ 1	Misc.HackTool.AutoKMS	Trojan	570,692
4	↓ 1	Trojan.Agent.gen	Trojan	502,322
5	-	Trojan.ShadowBrokers.A	Trojan	359,143
6	↑ 2	Trojan.HTML.Ramnit.A	Trojan	331,096
7	↓ 1	Misc.HackTool.KMSActivator	Trojan	298,196
8	↓ 1	Gen:Variant.Razy.107843	Trojan	257,152
9	New	Gen:Variant.Graftor.687683	Trojan	206,040
10	↑ 3	Win32.Neshta.A	Virus	160,943
11	↑ 1	Gen:Variant.Razy.553929	Trojan	160,115
12	New	Gen:Variant.Ulise.104992	Trojan	159,613
13	↓ 3	Misc.Riskware.TunMirror	Trojan	157,404
14	↓ 5	Misc.Keygen	Trojan	154,330
15	New	Exploit.CVE-2010-2568.Gen	Exploit	98,152

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 04 월 01 일 ~ 2020 년 04 월 30 일

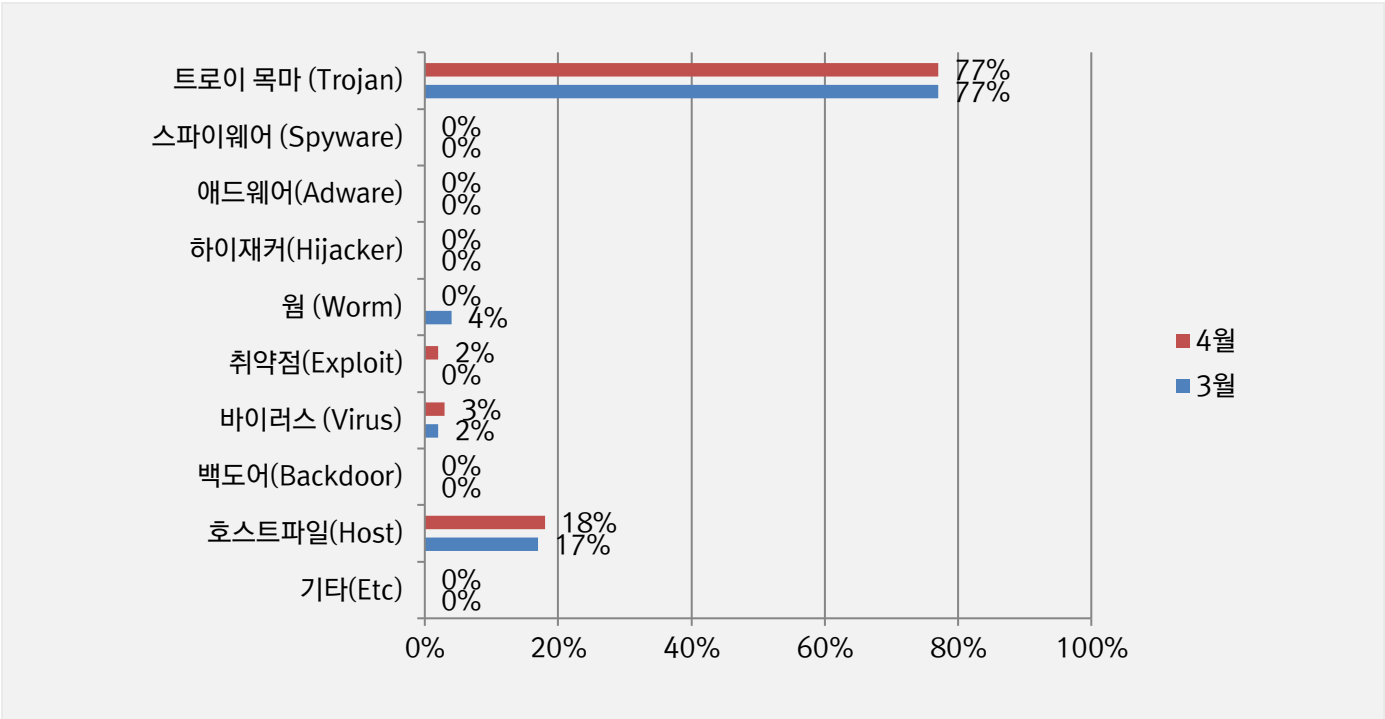
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 77%를 차지했으며 호스트파일(Host) 유형이 18%로 그 뒤를 이었다. 전반적으로 3 월에 비해 전체 감염건수는 거의 유사한 수준이었다.



카테고리별 악성코드 비율 전월 비교

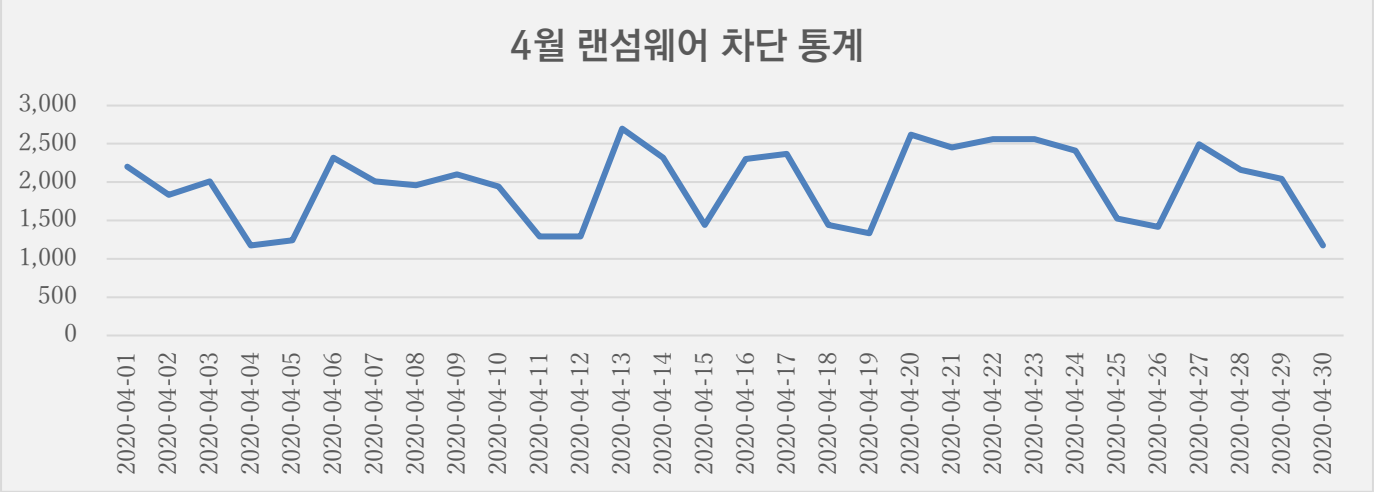
3 월에는 2 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 증가했으며, 호스트파일(Host) 유형 악성코드 비율 역시 소폭 증가했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

4 월 랜섬웨어 차단 통계

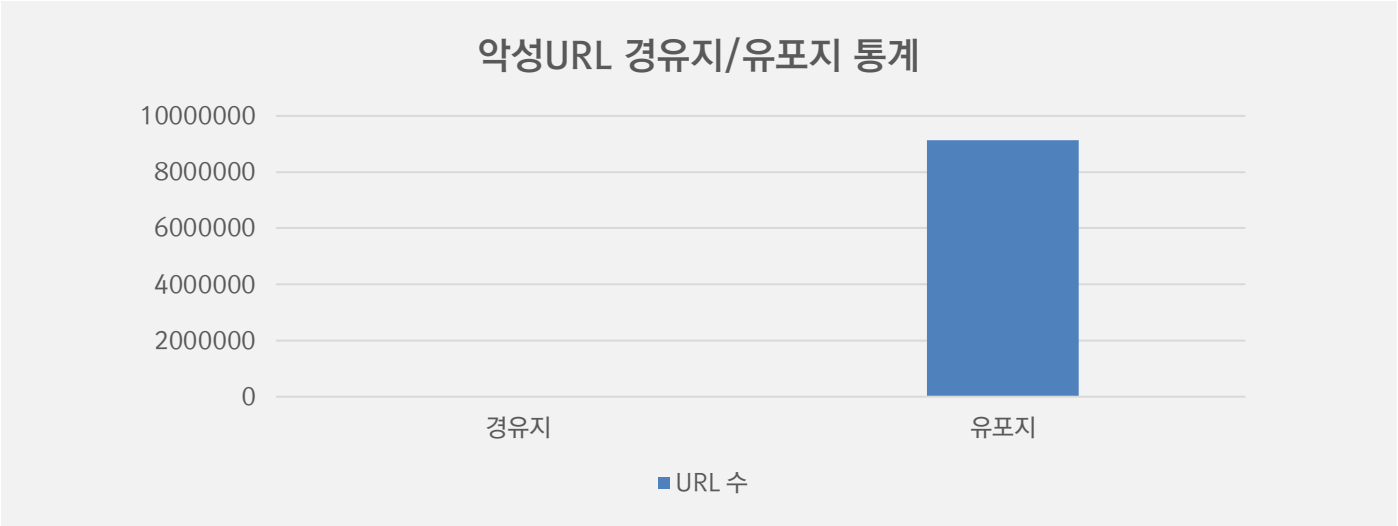
해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 4 월 1 일부터 4 월 30 일까지 총 58,739 건의 랜섬웨어 공격시도가 차단되었다. 3 월에 비해 랜섬웨어 공격건수는 약 5%가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 4 월 한달간 총 9,158,087 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 3 월 한달 간 확인되었던 5,230,770 건의 악성코드 경유지/유포지 URL 수에 비해 75% 이상 크게 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 봐주기 바란다.



02

전문가 보안 기고

1. 통일 정책분야 연구원으로 사칭한 ‘금성 121’ APT 공격 주의

2. 코로나 19 '긴급재난지원금 신청' 노린 스미싱 공격 본격화 예상돼

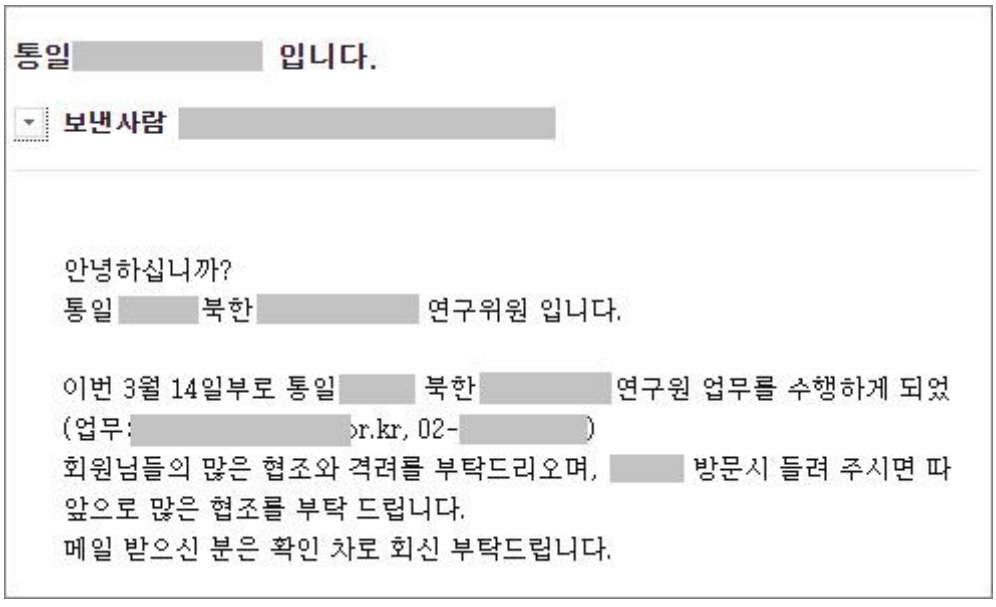
1. 통일 정책분야 연구원으로 사칭한 '금성 121' APT 공격 주의

최근 특정 정부가 연계된 것으로 알려진 사이버 위협 그룹 일명 '금성 121(Geumseong121)' 해커들이 새로운 공격 시나리오로 APT(지능형지속위협) 공격을 시도한 정황이 포착되어 주의가 요구됩니다.

금성 121 그룹은 최근까지 다양한 해킹 사례의 배후로 지목되고 있으며, 라자루스(Lazarus), 김수키(Kimsuky), 코니(Konni) 등과 함께 대한민국을 주무대로 활동하는 대표적인 위협 조직 중 하나입니다.

최근 포착된 APT 공격에서는 이들은 통일정책 분야의 연구원으로 변장해 공격 대상의 스마트폰 전화번호 등 개인정보를 1 차 수집하고 일정 기간 후 상대방과 성별이 다른 카카오톡 프로필을 만들어 해킹을 시도하고 있음이 확인되었습니다. 만약 공격 대상자가 남성일 경우에는 미모의 여성 사진과 이름으로 접근해, 미인계 작전을 통해 공격을 진행한 것으로 보여집니다.

공격자는 먼저 대북 분야에서 활동하는 주요 인사들을 선별하고, 이들에게 자신이 통일 정책 분야의 기관에 새로 근무하게 된 여성 선임연구원처럼 사칭한 가짜 소개 이메일을 보냅니다.


통일 [redacted] 입니다.

보낸사람 [redacted]

안녕하십니까?
통일 [redacted] 북한 [redacted] 연구위원 입니다.

이번 3월 14일부로 통일 [redacted] 북한 [redacted] 연구원 업무를 수행하게 되었
(업무: [redacted] r.kr, 02- [redacted])
회원님들의 많은 협조와 격려를 부탁드리오며, [redacted] 방문시 들려 주시면 따
앞으로 많은 협조를 부탁 드립니다.
메일 받으신 분은 확인 차로 회신 부탁드립니다.

[그림 1] 통일정책분야 연구원으로 위장하여 관련업계 관계자들에게 보낸 악성 이메일 화면

02 전문가 기고

해당 이메일에는 기존 스피어 피싱 공격처럼 별도의 악성 파일이나 위험한 URL 링크를 포함하지 않고 평범한 소개 및 인사 내용만을 담고 있어 메일 수신자로 하여금 해킹 의심을 최소화하고 있습니다. 그러나 이후 이메일을 수신한 다수의 사람에게 확인차 회신을 요청하고, 일부 답신한 사람들에게 연락 목적으로 전화번호 등을 요구합니다.

이런 일반적인 이메일 소통 과정을 통해 공격 대상자의 스마트폰 전화번호를 확보하고, 일정 기간이 지난 다음 가상의 새로운 인물로 위장해 카카오톡으로 은밀히 접근을 시도합니다.

카카오톡을 통해 공격 대상자와 접촉한 공격자는 최소 1 달 이상 극히 일상적인 대화와 정상적인 사진, 문서 파일 등을 여러 차례 공유하며 최대한 의심을 피하며 대화를 지속합니다. 이를 통해 자신이 보낸 파일은 전혀 보안 위협이 되지 않는 것처럼 위장하고, 점차 신뢰하도록 장기간 치밀한 과정을 거치게 됩니다.

이러한 생활 밀착형 개인 소통을 통해 어느정도 친밀감을 높이고 안심했다고 생각하는 시점에 공격자는 드디어 본색을 드러내고, 위협요소가 포함된 자료를 전달해 해킹을 본격적으로 수행하게 됩니다.

온라인상 불특정 인물과 인맥을 맺는데 있어 각별히 주의가 필요해 보이는 부분입니다.

특정 정부 후원을 받는 '금성 121' 조직은 기존의 PC 기반 공격뿐만 아니라 이처럼 스마트폰을 활용하여 다양한 형태의 APT 공격을 시기적절하게 수행하고 있으며, 1 회성이 아닌 중장기적인 플랜과 시간을 두고 맞춤형 APT 공격을 수행하고 있는 것으로 판단됩니다.

실제로 이 조직은 지난 3 월 '오퍼레이션 스파이 클라우드(Operation Spy Cloud)' APT 공격을 통해 외교, 통일, 안보분야 종사자나 대북관련 단체장, 탈북민을 겨냥한 위협을 가속화 중인 것이 알려진 바 있고, 웹 서버를 직접 디자인해 구축하는 등 갈수록 치밀하고 과감한 공격을 수행한 사실도 확인되었습니다. 특히, 구글 플레이 공식 앱 마켓이나 유튜브를 통한 신뢰 기반의 공격 대담성은 다른 APT 조직에서 흔히 보기 어려운 독특함을 지니고 있습니다.

'금성 121' 조직은 한국의 정치적인 상황과 맞물려 통일 및 대북 관련 관계자를 겨냥한 대표적인 위협 배후로 지목되고 있으며, 다양한 모바일 서비스를 활용한 위협 활동을 지속하고 있습니다. 특히 최근까지 모바일 기반으로 공격 대상자를 선별해 공격을 진행하고 있는 상황을 봤을 때, 모르는 사람이 대화를 시도해 올 경우 함부로 친구 관계를 맺지 않도록 하고, 반드시 별도의 신분 확인 과정을 거치는 등의 보안 의식 생활화가 필요합니다.

2. 코로나 19 '긴급재난지원금 신청' 노린 스미싱 공격 본격화 예상돼

코로나 19 위기 극복을 위한 정부 지원인 긴급재난지원금 신청이 지난 5 월 11 일부터 시작되며 많은 관심이 집중되고 있는 가운데, '긴급재난지원금 조회 및 안내'를 사칭한 스미싱 공격이 등장했습니다.

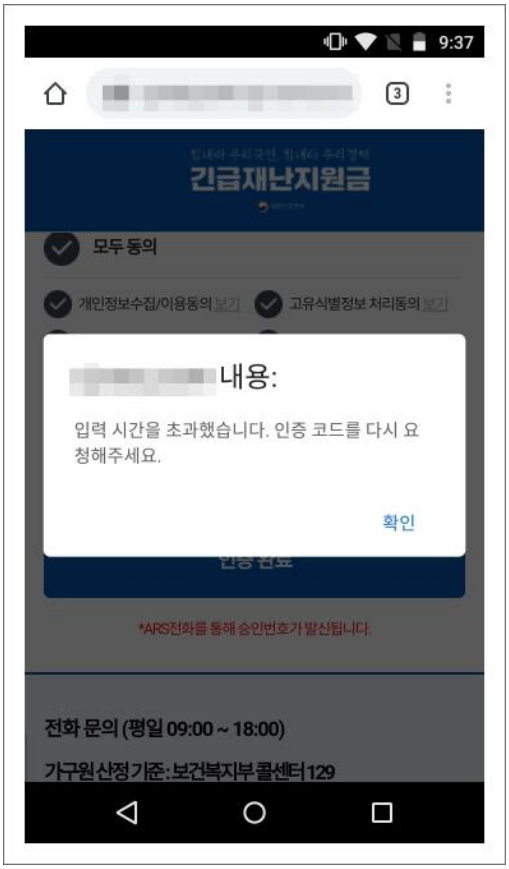
[그림 1] 정부 긴급재난지원금 사이트로 위장된 피싱 사이트

ESRC 에서는 12 일 정부 긴급재난지원금 신청 이슈를 노린 스미싱 공격을 확인했습니다. 발견된 스미싱은 11 일 오후부터 다수 유포되었으며, 문자 메시지 내용은 스미싱 공격자가 주로 사용하던 택배 사칭 메시지가 그대로 재활용되었습니다.

스미싱 문자에는 '주소가 불분명하여 배달이 불가능하다'는 택배 사칭 내용이 적혀있으며, 문자에 첨부된 인터넷 주소(URL)를 클릭하면 공격자가 미리 제작해둔 가짜 '정부 긴급재난지원금 신청' 사이트로 이동됩니다.

만약 사용자가 가짜 긴급재난지원금 신청 사이트에 자신의 개인정보를 입력 후 인증번호 요청 버튼을 클릭하면, 입력된 개인정보는 고스란히 공격자에게 넘어가게 됩니다.

[그림 2] 가짜 긴급재난지원금 페이지에서 개인정보를 수집하는 화면



[그림 3] 인증번호 요청 클릭 후 일정시간 지나면 입력 시간 초과 메시지 띄움

02 전문가 기고

이번 공격의 특이점은 공격자가 정교하게 가짜 정부 긴급재난지원금 신청 사이트를 제작해 두었음에도 불구하고, 재난지원금 신청 유도 내용이 아닌 '택배 사칭' 내용의 문자 메시지(SMS)를 발송했다는 점입니다.

실제로 공격이 발견된 지 일정 시간이 흐른 5 월 12 일 오전 6 시까지도 '택배 사칭' 스미싱에 가짜 정부 긴급재난지원금 신청 사이트로 연결되는 URL 이 포함돼 유포되고 있는 것으로 확인되었습니다.

ESRC 에서는 공격자가 택배 사칭 내용으로 스미싱 문자를 보낸 것은 실수로 추측하고 있으며, 언제든지 실수를 바로잡고 정부 긴급재난지원금 수령 신청과 관련된 내용의 스미싱 문자를 보낼 수 있다고 추정하고 있습니다.

**업데이트(5/12 14:00)

택배 사칭 스미싱 내용이 '전국민코로나 19 위기극복을위한 긴급재난지원금 조회 및 안내 서비스' 내용으로 수정되어 공격이 이뤄지고 있는 것이 확인되었습니다. 실수로 나갔던 메시지가 수정된 것으로 보입니다.

현재 긴급재난지원금과 관련된 전 국민의 관심이 높아진 만큼, 출처가 불분명한 번호로부터 유사한 내용의 문자 메시지를 수신하게 된다면 더욱 각별히 주의를 기울여야 합니다.
지난 몇 달간 '마스크 무료 수령, 재난지원금 상품권' 등의 코로나 19 키워드를 활용한 스미싱이 수차례 발견되었고, 새로 등장한 '긴급재난지원금 신청' 사례 역시 유사한 사회공학적 기법을 적절히 결합했음을 확인할 수 있습니다.

공격자들이 5 월 11 일부터 시작된 긴급재난지원금 온라인 신청 기간을 시기 적절하게 노려 이용자들을 현혹하고 있어, 모바일 보안 강화가 요구되고 있는 시점입니다.

03
악성코드 분석 보고

[Trojan.Ransom.Makop] 악성코드 분석 보고서

최근 국내 기업에 이력서 확인 메일로 'Trojan.Ransom.Makop'(이하 Makop 랜섬웨어)가 유포되고 있다. 공격자는 아래의 메일을 통해 이용자에게 '이력서.tar' 첨부파일 실행을 유도한다. Makop 랜섬웨어는 파일 암호화 기능을 수행하는 악성코드이다.

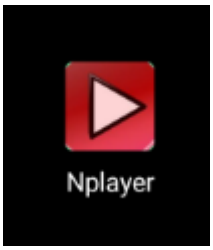
[그림] 이력서 위장 메일

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.Makop' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.SmsSpy] 악성코드 분석 보고서

해당 악성 앱은 N 번 방 동영상 이슈를 활용한 스미싱을 통해서 유포되었다. 동영상 이슈를 활용하는 만큼 'Nplayer'라는 앱 명을 사용한다. 특히, 처음 실행 시 특정 성인 사이트를 로드하여 팝업함으로써 사용자를 속임과 동시에 기기 및 문자 정보를 탈취한다.




```
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.DEVICE_POWER" />
```

[그림] 앱 특징

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

04
글로벌 보안 동향

NSA, 웹 셸을 심는데 흔히 악용되는 취약점 목록 공개

NSA shares list of vulnerabilities commonly exploited to plant web shells

미 국가안보국(NSA)와 호주 통신보안국(ASD)이 기업들에 웹 대면 서버 및 내부 서버에서 일반 웹 셸을 찾아볼 것을 경고하는 보안 권고를 발행했다. 웹 셸은 오늘날 가장 널리 사용되는 악성코드 유형 중 하나다. "웹 셸"이라는 용어는 해킹된 서버에 설치된 악성 프로그램이나 스크립트를 의미한다. 웹 셸은 해커가 해킹된 서버 및 파일 시스템을 조작하는데 사용할 수 있는 비쥬얼 인터페이스를 제공한다. 웹 셸 대부분에는 서버에서 해커가 사용 가능한 파일의 이름 변경, 복사, 이동, 편집 기능 및 새로운 파일 업로드 기능 등이 포함되어 있다. 파일 및 디렉토리의 권한을 변경하거나 서버에서 데이터를 압축 및 다운로드하는 것도 가능하다. 해커들은 인터넷에 노출된 서버 또는 애플리케이션(CMS, CMS 플러그인, CMS 테마, CRM, 인트라넷, 기타 기업 앱 등)에 존재하는 취약점을 악용하여 웹 셸을 설치한다.

웹 셸은 Go 부터 PHP 까지 모든 언어로 작성될 수 있다. 이를 통해 해커가 일반적인 이름(index.asp 또는 uploader.php 등)을 사용하여 모든 웹사이트의 코드에 웹 셸을 숨기는 것이 가능해져 사람이 웹 방화벽이나 웹 악성코드 스캐너의 도움을 받지 않고 탐지해 내는 것이 거의 불가능하다. 마이크로소프트는 2020 년 2 월 보고서를 발표해 77,000 건의 활성화된 웹 셸이 발견했으며, 웹 셸을 오늘날 가장 널리 사용되는 악성코드 타입 중 하나로 꼽았다.

내부 네트워크의 백도어 역할이 가능한 웹 셸

하지만 많은 기업들은 시스템에 웹 셸이 설치될 경우 발생하는 위험에 대해 완벽히 이해하고 있지 않은 것으로 보인다. 기본적으로 웹 셸은 백도어의 역할을 하며 최우선 순위로 처리되어야 한다. NSA 와 ASD 는 보안 권고를 통해 종종 무시되고 있는 이 공격 벡터에 대한 위험을 다시 한번 상기시켰다.

"웹 셸은 다른 시스템에 공격자의 명령을 전달하기 위한 영구 백도어나 릴레이 노드의 역할을 할 수 있다. 공격자는 네트워크에서 트래픽을 라우팅하기 위해(예: 인터넷 대면 시스템에서 내부 네트워크로)해킹된 시스템의 웹 셸 다수를 연결시켜 사용한다."

이 두 기관은 관리자가 이러한 위협을 탐지 및 대응하는데 사용할 수 있는 툴을 포함한 17 페이지 보고서 [PDF]를 공개했다. 이 보고서에는 다음 내용이 포함된다.

- 제품 웹사이트를 정상 이미지와 비교할 수 있는 스크립트
- 웹 트래픽에서 비정상 URL을 탐지할 수 있는 Splunk 쿼리
- IIS 로그 분석 툴
- 일반적인 웹 셸의 네트워크 트래픽 시그니쳐
- 예기치 않은 네트워크 플로우를 식별하는 방법

- Sysmon 데이터에서 비정상 프로세스 호출을 식별하는 방법
- Auditd에서 비정상 프로세스 호출을 식별하는 방법
- 웹 액세스 가능 디렉토리에서 변경을 막는 HIPS 룰
- 흔히 악용되는 웹 애플리케이션 취약점 목록

위에 언급된 툴은 NSA 의 GitHub 프로필에서 찾아볼 수 있다. 이 권고에 포함된 모든 조언과 툴도 훌륭하지만, 시스템 관리자는 이미 해킹된 호스트를 검색하기 전 먼저 시스템을 패치하는 것이 좋다. NSA 와 ASD 가 공개한 흔히 악용되는 서버 소프트웨어 목록에서부터 패치를 해야하며, 해당 목록에는 Microsoft SharePoint, Microsoft Exchange, Citrix, Atlassian Confluence, WordPress, Zoho ManageEngine, Adobe ColdFusion 등과 같은 인기있는 툴이 포함되어 있다. 'n-day' 취약점으로 인한 위험에 대응하기 위해 인터넷 대면 및 내부 웹 애플리케이션 모두를 신속히 패치해야 한다.

[출처] https://www.zdnet.com/article/nsa-shares-list-of-vulnerabilities-commonly-exploited-to-plant-web-shells/
https://media.defense.gov/2020/Apr/22/2002285959/-1/-1/0/DETECT%20AND%20PREVENT%20WEB%20SHELL%20MALWARE.PDF
https://github.com/nsacyber/Mitigating-Web-Shells

VMWare, 치명적인 vCenter 서버 취약점 수정

VMWare releases fix for critical vCenter Server vulnerability

VMware 가 vCenter 서버 가상 인프라 관리 플랫폼에 존재하는 치명적인 취약점을 수정하는 보안 업데이트를 공개했다. 공격자가 이를 악용할 경우 민감 정보에 접근하고 가상 어플라이언스 또는 윈도우 시스템을 제어할 수 있었다. IT 관리자는 vCenter Server 를 통해 기업 환경 내 가상화 호스트 및 가상 머신을 단일 콘솔을 통해 중앙 집중식으로 관리할 수 있다. 관리자 한 명이 워크로드 수백 개를 관리하며 물리 인프라를 관리하는 것보다 생산성을 두 배 이상 높일 수 있다. 미국의 사이버 보안 및 인프라 보안국 (CISA)는 경고를 발행해 "공격자가 이 취약점을 악용할 경우 취약한 시스템을 제어할 수 있다"라고 밝히며 사용자 및 관리자에게 업데이트를 적용할 것을 권장했다.

CVSSv3 10 점 만점을 기록한 치명적인 취약점

VMware 의 보안 권고에 따르면, 비공개로 제보된 이 취약점은 CVE-2020-3952 로 등록되었으며 CVSSv3 기본 점수 만점인 10 점을 기록했다. 이 보안 이슈는 업그레이드되어 설치된 VMWare Directory Service (vmdir)에만 존재하며 액세스 제어가 잘못 구현되었기 때문에 발생한다. 6.7u3f 이전 버전의 vCenter Server 6.7 (내장 또는 외장 PSC)이 이전 릴리스 라인인 6.0 또는 6.5 에서 업그레이드된 경우 CVE-2020-3952 에 취약한 것으로 나타났다. 새로 설치된 vCenter Server 6.7 (내장 또는 외장 PSC)는 영향을 받지 않는다.

VMware 는 일부 조건에서 VMware vCenter Server 와 함께 내장 또는 외장 PSC(Platform Service Controller)의 일부로 제공되는 vmdir 에 액세스 제어가 제대로 구현되지 못했다며, 설치된 취약한 vmdir 로의 네트워크 접근 권한이 있는 악성 공격자는 매우 민감한 정보를 추출할 수 있을 가능성이 있다고 밝혔다. 이는 인증 시 vmdir 에 의존하는 vCenter Server 및 기타 서비스를 해킹하는데 사용될 수 있다. 설치된 vCenter Server 가 CVE-2020-3952 취약점에 영향을 받는지 확인하고자 할 경우에는 KB78543 문서를 참고하면 된다.

완화 조치

이 보안 취약점은 매우 치명적이기 때문에 가능한 한 빨리 vCenter Server 를 업그레이드할 것을 강력히 권장한다. 이 취약점을 윈도우나 가상 어플라이언스에서 패치하려면 vCenter Server 6.7u3f 로 업그레이드해야 한다. VMware 는 지난달 또 다른 보안 업데이트를 발행해 VMWare Workstation Pro 의 치명적인 취약점을 수정했다. 공격자가 이를 악용할 경우 서비스 거부(DoS) 공격을 수행하거나 해당 윈도우 호스트에서 명령을 실행할 수 있었다. 그로부터 4 일 후, VMware 는 또다시 VMware Workstation, Fusion, VMware Remote Console, Horizon Client 에서 심각도 '높음'인 권한 상승 취약점 및 DoS 결함을 패치했다.

[출처] https://www.bleepingcomputer.com/news/security/vmware-releases-fix-for-critical-vcenter-server-vulnerability/

https://www.us-cert.gov/ncas/current-activity/2020/04/10/vmware-releases-security-updates-vmware-directory-service

https://www.vmware.com/security/advisories/VMSA-2020-0006.html

https://kb.vmware.com/s/article/78543

인터폴, 병원에 대한 랜섬웨어 공격이 증가하고 있다고 경고

Interpol: Ransomware attacks on hospitals are increasing

인터폴이 현재 코로나 바이러스가 성행함에도 불구하고 랜섬웨어를 이용해 병원을 공격하고 있다고 경고했다. 다양한 랜섬웨어 변종 운영자들은 지난달 BleepingComputer 측에 코로나 바이러스 팬데믹으로 인해 건강 및 의료 관련 조직은 공격하지 않을 것이라 밝혔지만, 놀라운 일은 아니다.

Maze 랜섬웨어는 의료 시설을 공격하지 않겠다고 선언하기 전 약품을 검사하는 회사로부터 훔친 데이터를 공개했으며, Ryuk 은 병원이 매일 새로운 코로나 바이러스 환자로 북새통을 이루는 와중에도 지속적으로 의료 기관을 공격했다. 러시아어를 구사하는 공격자들 또한 유럽의 제약 및 제조 회사 2 곳에 랜섬웨어 공격을 가했다.

지난주, 마이크로소프트는 REvil(Sodinokibi) 랜섬웨어 공격을 예방하기 위해 병원 수십 곳에 네트워크 상의 VPN 기기와 게이트웨이가 취약한 채 노출되어 있다는 경고를 보냈다. 인터폴의 사이버 범죄 위협 대응 팀은 "바이러스에 대응하고 있는 핵심 조직과 인프라에 대한 랜섬웨어 공격 시도가 급격히 증가하고 있음을 발견했다"라고 경고했다. 또한 194 개 회원국의 경찰에 "퍼플 노티스(Purple Notice)"를 발행하여 랜섬웨어 위협을 높였다고 밝혔다.

병원을 노린 공격, 사람의 목숨 위협해

인터폴의 사이버범죄 위협 대응(CTR) 팀은 현재 코로나 바이러스와 관련된 사이버 위협에 대한 더 많은 정보를 수집하고, 랜섬웨어의 공격 대상이 된 조직에 도움을 주기 위해 노력하고 있다. 또한 회원국의 법 집행기관과 긴밀히 협업하여 랜섬웨어 공격 사례를 조사하고 위협 데이터를 분석하여 위험을 완화하기 위한 노력을 하고 있다. 인터폴의 사무총장인 Jurgen Stock 는 아래와 같이 발표했다. "병원의 중요 시스템을 잠글 경우 코로나 바이러스 대응에 필요한 의료 대응이 지연될 뿐만 아니라 환자의 사망으로 이어질 수 있다. 인터폴은 회원국이 언제든 도움을 요청할 수 있도록 대기 중이며, 중요한 의료 시스템을 공격하지 못하도록 모든 지원을 제공하며, 이를 노리는 공격자들을 체포하기 위해 노력할 것이다."

[이미지 출처] https://twitter.com/INTERPOL_HQ/status/1246376755985694720

랜섬웨어 공격으로부터 보호하는 법

현재 의료 조직의 네트워크가 랜섬웨어 공격의 대상이 되고있다. 이 공격은 악성코드 페이로드를 포함한 파일을 첨부한 이메일을 발송하는 스팸 캠페인을 통해 이루어 진다. 공격자들은 이러한 악성 첨부파일을 보건 기구 또는 정부에서 발행한 코로나바이러스에 대한 중요한 정보가 포함된 문서로 위장한다. 인터폴은 이러한 공격에 대응하기 위해 아래와 같은 조치를 취할 것을 권장했다.

- 신뢰할 수 있는 출처로부터 받은 이메일이나 소프트웨어/애플리케이션만 오픈하기
- 알 수 없는 발신자나 예상치 못한 이메일의 링크 또는 첨부파일 오픈하지 않기
- 이메일 시스템을 스팸으로부터 보호하기
- 모든 중요한 파일을 정기적으로 백업하고 시스템과 분리하여 저장하기 (클라우드, 외장하드 등)
- 최신 안티바이러스 소프트웨어가 모든 시스템에 설치되어 있고 지속적으로 실행하고 있는지 확인하기
- 모든 시스템에서 강력하고 고유한 패스워드를 사용하고 정기적으로 변경하기

[출처] https://www.bleepingcomputer.com/news/security/interpol-ransomware-attacks-on-hospitals-are-increasing/

(주)이스트시큐리티

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