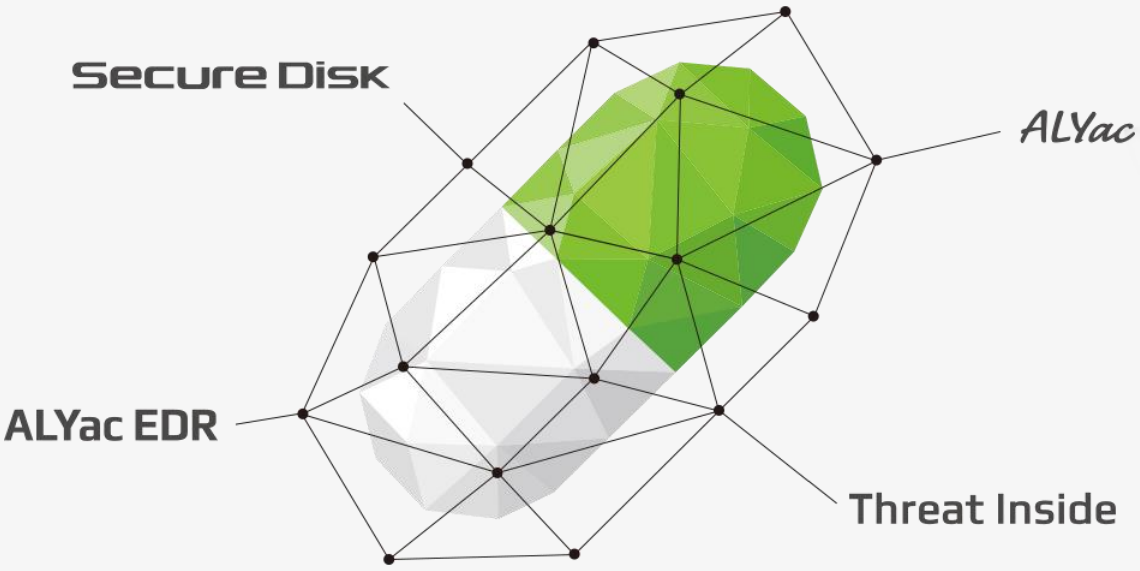
이스트시큐리티

보안 동향 보고서

No.126 2020.03



No.126 2020.03

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 2 월에는 RAT 을 포함한 다양한 악성코드가 발견되었고 그 외에도 다양한 프로토콜, 장비취약점을 악용한 공격이 확인되었습니다. 그러나 무엇보다도, 1 월 말경부터 전 세계적으로 이슈가 되고 있는 '코로나바이러스' 관련 키워드를 악용한 공격들이 2 월 동안 집중적으로 확인되었습니다.

이 부분은 신종 코로나바이러스의 확진자가 지속해서 발생하면서, 신종 코로나바이러스에 대한 대중의 관심과 우려도 커지고 있기 때문에 공격자들은 이런 상황에서 대중들의 호기심과 공포 심리를 이용하여 악성코드를 유포하려는 시도를 지속해서 수행하고 있는 것으로 보입니다.

최근 발견된 악성코드 중 corona virus 명칭이 포함된 파일명의 윈도/안드로이드 악성코드로 유포가 대량으로 이뤄지고 있습니다. 이들은 주로 이메일 첨부파일을 통해 악성코드를 유포 중이며, 공격자들이 유포한 악성코드들의 명칭에는 공통으로 coronavirus 라는 키워드가 포함되어 있습니다.

이들은 CDC, WHO, 혹은 코로나바이러스연구자로 사칭하여 사용자들이 궁금해할 만한 지역감염현황, 감염대책, 예방법, 상세한 코로나바이러스 연구 진행 상황 등을 보여주는 것처럼 꾸미고 있기 때문에 전 세계 불특정 개인들뿐만 아니라 관련 기관/기업들도 동시에 타깃팅 하고 있는 상황입니다.

공격자들이 코로나바이러스 키워드를 통해 유포하는 악성코드의 종류는 다양합니다. 랜섬웨어, 백도어, 인포스틸러 등 많은 종류의 악성코드가 확인되고 있습니다. 코로나 19 내용으로 가장한 김수키(Kimsuky)조직의 스모크스크린 APT 공격 역시 포착되기도 했습니다. 또한 관련 키워드를 다루는 피싱 공격도 계속 이어지고 있으므로 주의를 기울여야 합니다.

코로나 19 바이러스 사태 이후, 많은 기업들이 바이러스 확산을 막고 예방하고자 재택근무를 수행 중에 있습니다. 재택근무 중 대다수는 사내망 접속을 외부에서 수행하기 위해 VPN 을 통해 사내망에 접속하게 되는데 이때 재택근무를 위해 사용하고 있는 장비에 대한 보안이 매우 중요합니다. 재택근무를 위해 사용하는 장비들에 대한 최신 보안업데이트 유지 및 불필요한 프로그램 삭제, 그리고 알약과 같은 안티바이러스 솔루션을 최신 DB 업데이트&실시간감시기능 활성화 상태로 사용해 주셔야 합니다.

또한 불필요한 외부메일 수신 시 열람을 자제하고 반드시 사내 보안팀에 신고하시거나 저희 ESRC 쪽에 공유해주셔야 안전함을 꼭 기억해주시기 바랍니다.

코로나 19 로부터 안전하고 건강하시길 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 2 월의 감염 악성코드 Top 15 리스트에서는 지난 2020 년 1 월에 3 위를 차지했었던 Hosts.media.opencandy.com 가 새롭게 1 위를 차지했으며, 1 월에 각각 1 위와 2 위를 차지했던 Misc.HackTool.AutoKMS 와 Trojan.Agent.gen 이 이번 달, 한계단씩 떨어진 순위를 기록했다. Hosts.media.opencandy.com 은 주로 토렌트 프로그램을 최소 설치할 때 함께 설치되는 추가 제휴 프로그램을 통해 일부 호스트파일 내용이 변경되고 지속적으로 또다른 추가 제휴 프로그램이 설치되게 한다.

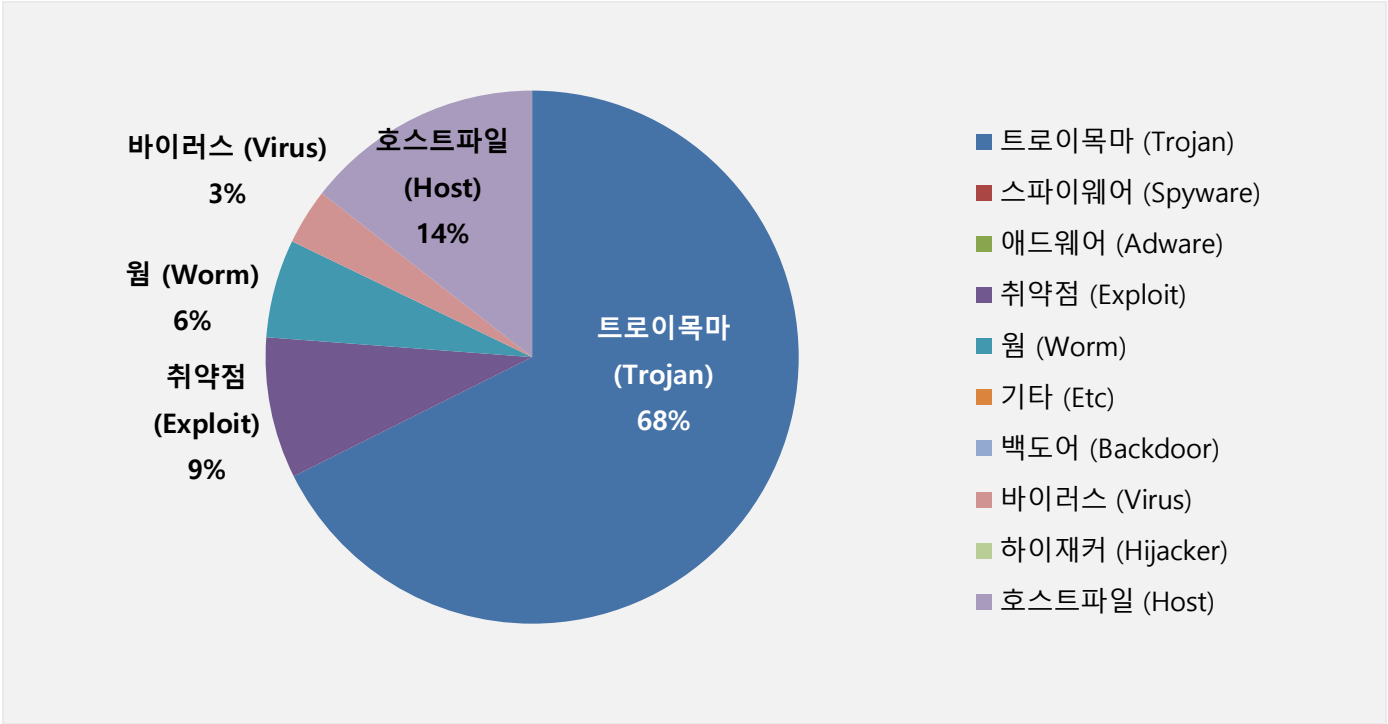
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 2	Hosts.media.opencandy.com	Host	654,589
2	↓ 1	Misc.HackTool.AutoKMS	Trojan	578,284
3	↓ 1	Trojan.Agent.gen	Trojan	560,235
4	↑ 1	Trojan.ShadowBrokers.A	Trojan	512,921
5	↑ 4	Exploit.CVE-2010-2568.Gen	Exploit	387,859
6	↑ 1	Misc.HackTool.KMSActivator	Trojan	310,628
7	↑ 3	Trojan.HTML.Ramnit.A	Trojan	283,498
8	-	Gen:Variant.Razy.553929	Trojan	222,162
9	New	Misc.Riskware.BitcoinMiner	Trojan	168,725
10	↑ 2	Misc.Riskware.TunMirror	Trojan	167,421
11	New	Worm.ACAD.Bursted.doc.B	Worm	162,789
12	↓ 1	Misc.Keygen	Trojan	161,540
13	↑ 2	Win32.Neshta.A	Virus	153,228
14	-	Worm.ACAD.Bursted	Worm	107,117
15	New	JS:Trojan.Cryxos.2745	Trojan	95,190

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 02 월 01 일 ~ 2020 년 02 월 29 일

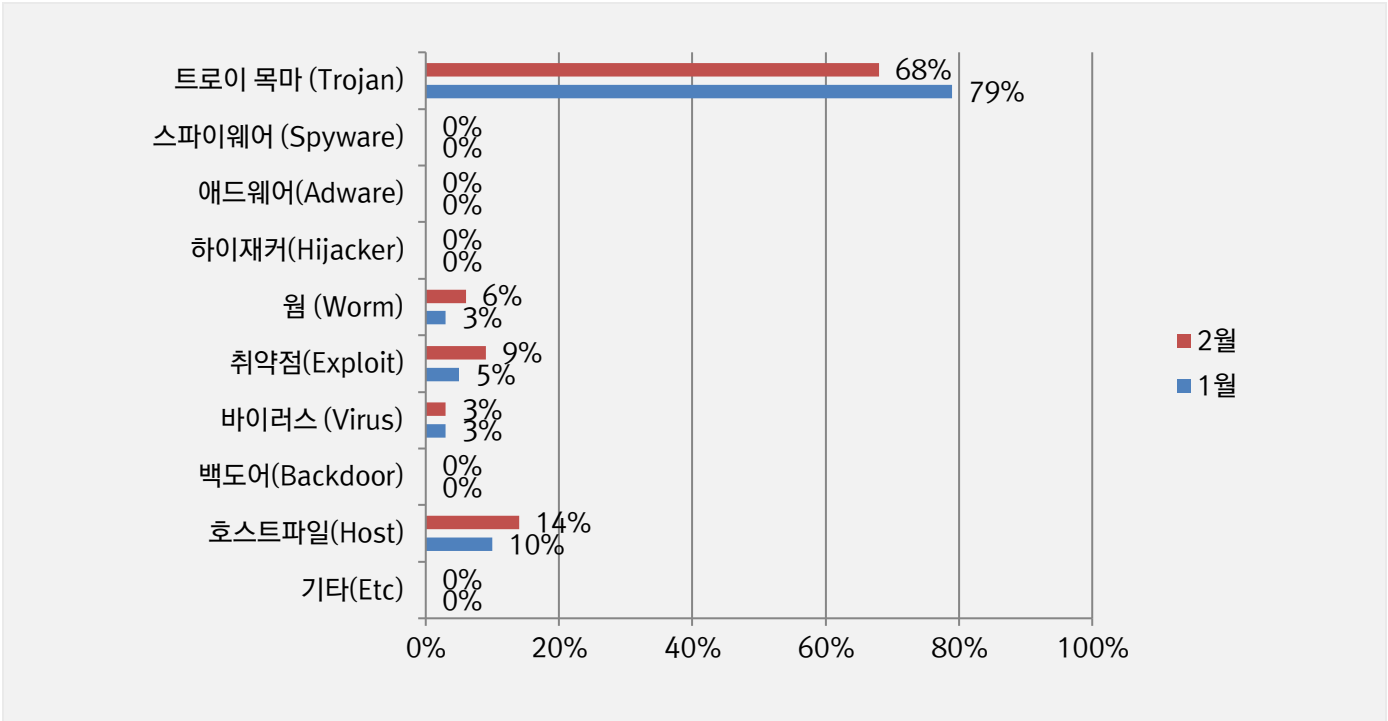
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 68%를 차지했으며 호스트파일(Host) 유형이 14%로 그 뒤를 이었다. 전반적으로 1 월에 비해 전체 감염건수는 1.3% 가량 소폭 증가했다.



카테고리별 악성코드 비율 전월 비교

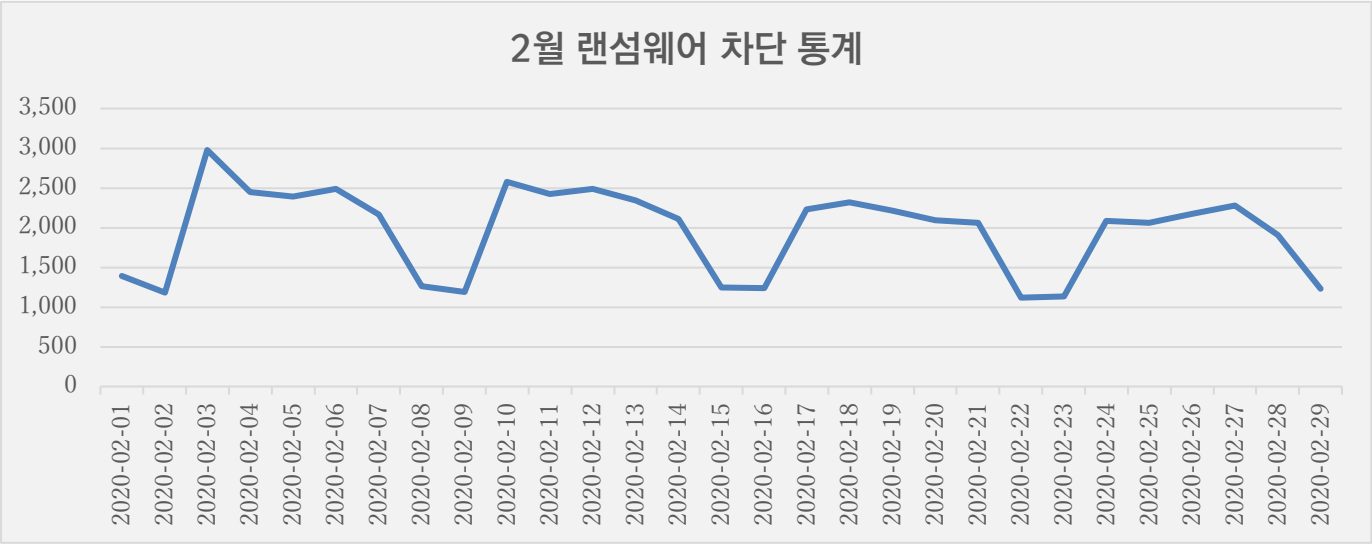
2 월에는 1 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 감소했으며, 호스트파일(Host) 유형 악성코드 비율이 크게 증가했다..



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

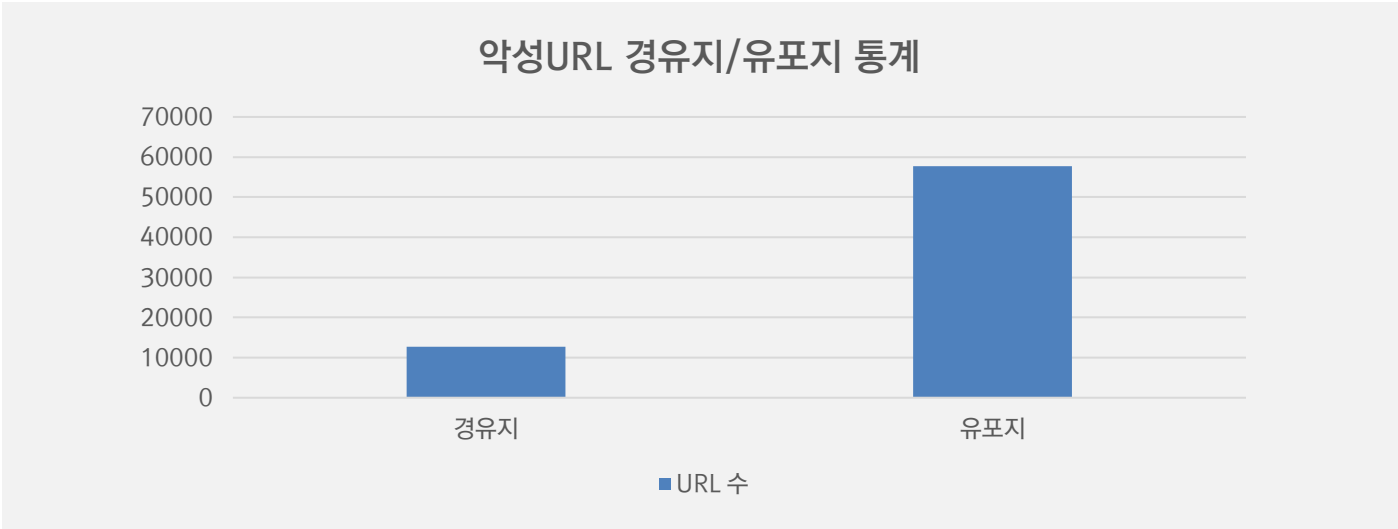
2 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 2 월 1 일부터 2 월 29 일까지 총 56,840 건의 랜섬웨어 공격시도가 차단되었다. 1 월에 비해 랜섬웨어 공격건수는 약 1.6% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 2 월 한달간 총 70,282 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 1 월 한달 간 확인되었던 192,628 건의 악성코드 경유지/유포지 URL 수에 비해 64% 정도 크게 감소한 수치다. 경유지 수치는 유포지 수치는 모두 크게 감소하였다. 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. 'Corona Ransomware'로 제품명을 변경한 Hakbit 랜섬웨어

2. 기업 내부 보안 위협하는 '섀도우 IT', 어떻게 대응해야 할까?

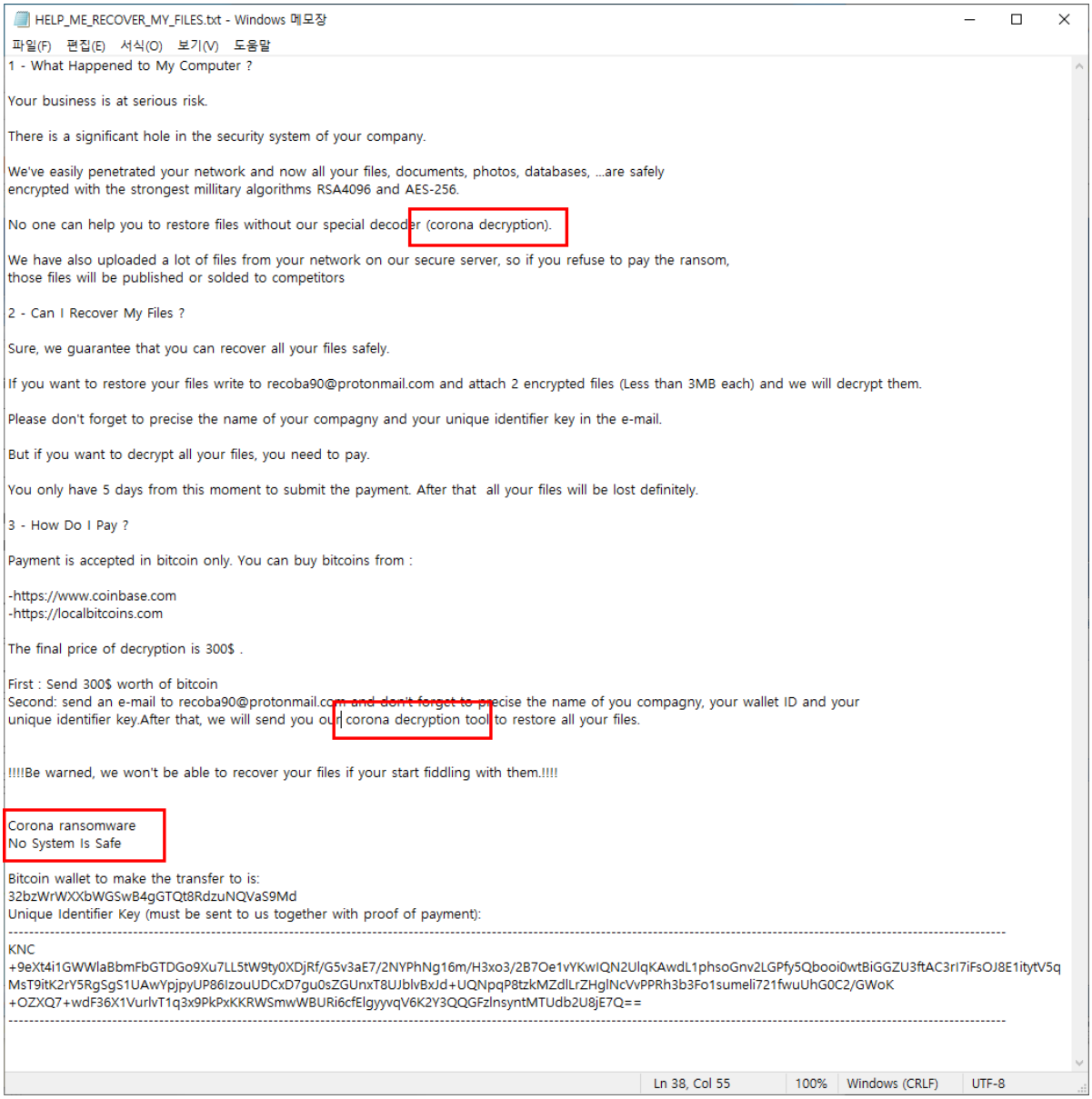
1.'Corona Ransomware'로 제품명을 변경한 Hakbit 랜섬웨어

최근 코로나 19 바이러스 감염증 확진자 수치가 계속 증가하고 있고, 대중들의 관심과 공포가 집중되고 있는 상황에서 코로나(Corona) 바이러스 이슈를 노리고 'Corona Ransomware'(이하 코로나 랜섬웨어) 라는 명칭을 사용하는 랜섬웨어가 등장하여 주의가 필요합니다.

해당 랜섬웨어는 완전히 새로운 형태는 아니며, 2019 년 11 월 경에 유포된 바 있는 Hakbit 랜섬웨어의 변종으로 추정됩니다.

실제로 이번에 발견된 코로나 랜섬웨어는 Hakbit 랜섬웨어와 동작방식에서 여러모로 유사한 부분이 확인됩니다. 또한 랜섬노트의 경우, 이번 코로나 랜섬웨어가 랜섬노트를 화면에 띄우는 방식을 비롯하여 요구하는 금액과 안내하는 비트코인 지불 사이트, 랜섬노트 내용 등에서 코로나 랜섬웨어가 Hakbit 랜섬웨어의 변종이라고 추정하고 있습니다.

이번 Corona 랜섬웨어에 감염될 경우 사용자에게 보여주는 랜섬노트의 내용에는 피해자가 공격자에게 돈을 지불하면 제공 받을 수 있는 decoder 를 'Corona decryption' 이라고 명명하고 있으며 랜섬노트 최하단에는 'Corona ransomware'라는 이름을 적시하고 있음을 확인할 수 있습니다.



[그림 1] 코로나 랜섬웨어 랜섬노트 화면

다음은 코로나 랜섬웨어 랜섬노트의 전문 텍스트입니다.

* 코로나 랜섬웨어 랜섬노트 전문

1 – What Happened to My Computer ?

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network and now all your files, documents, photos, databases, ...are safely encrypted with the strongest millitary algorithms RSA4096 and AES-256.

No one can help you to restore files without our special decoder (corona decryption).
We have also uploaded a lot of files from your network on our secure server, so if you refuse to pay the ransom, those files will be published or solded to competitors

2 – Can I Recover My Files ?

Sure, we guarantee that you can recover all your files safely.

If you want to restore your files write to recoba90@protonmail.com and attach 2 encrypted files (Less than 3MB each) and we will decrypt them.
Please don't forget to precise the name of your compagny and your unique identifier key in the e-mail.

But if you want to decrypt all your files, you need to pay.
You only have 5 days from this moment to submit the payment. After that all your files will be lost definitely.

3 – How Do I Pay ?

Payment is accepted in bitcoin only. You can buy bitcoins from :
-https://www.coinbase.com
-https://localbitcoins.com

The final price of decryption is 300$.

First : Send 300$ worth of bitcoin
Second: send an e-mail to recoba90@protonmail.com and don't forget to precise the name of you compagny, your wallet ID and your

unique identifier key.After that, we will send you our corona decryption tool to restore all your files.

!!!!Be warned, we won't be able to recover your files if your start fiddling with them.!!!!

Corona ransomware

No System Is Safe
Bitcoin wallet to make the transfer to is:
32bzWrWXXbWGSwB4gGTQt8RdzuNQVaS9Md
Unique Identifier Key (must be sent to us together with proof of payment):

이번 코로나 랜섬웨어는 이전 랜섬웨어들과 마찬가지로 감염자의 파일을 암호화 하여 이를 볼모로 금전을 요구합니다. 이번 랜섬웨어는 2020 년 1 월 30 일경 제작된 것으로 확인되며, 피해자에게 암호화한 파일에 대한 복구를 위해 300$가치의 비트코인 암호화폐 지불을 요구합니다.

대상 파일을 암호화하는 코드는 아래 화면과 같습니다. (AES256)

```
rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
rijndaelManaged.Padding = PaddingMode.Zeros;
rijndaelManaged.Mode = CipherMode.CBC;
CryptoStream cryptoStream = new CryptoStream(fileStream, rijndaelManaged.CreateEncryptor
  (), CryptoStreamMode.Write);
FileStream fileStream2 = new FileStream(string_0, FileMode.Open);
int num;
while ((num = fileStream2.ReadByte()) != -1)
{
    cryptoStream.WriteByte((byte)num);
}
fileStream2.Close();
cryptoStream.Close();
fileStream.Close();
```

[그림 2] 파일 암호화 코드

암호화 대상 확장자, 경로, 제외 경로는 아래와 같습니다.

***암호화 대상 확장자**

"txt", "jpeg", "gif", "jpg", "png", "php", "cs", "cpp", "rar", "zip", "html", "htm", "xlsx", "avi", "mp4", "ppt", "doc", "docx", "xlsx", "sxi", "sxw", "odt", "hwp", "zip", "rar", "tar", "bz2", "mp4", "mkv", "eml", "msg", "ost", "pst", "edb", "sql", "accdb", "mdb", "dbf", "odb", "myd", "php", "java", "cpp", "pas", "asm", "key", "pfx", "pem", "p12", "csr", "gpg", "aes", "vsd", "odg", "raw", "nef", "svg", "psd", "vmx", "vmdk", "vdi", "lay6", "sqlite3", "sqlitedb", "accdb", "java", "class", "mpeg", "djvu", "tiff", "backup", "pdf", "cert", "docm", "xlsm", "dwg", "bak", "qbw", "nd", "tlg", "lgb", "pptx", "mov", "xdw", "ods", "wav", "mp3", "aiff", "flac", "m4a", "csv", "sql", "ora", "mdb", "mdf", "ldf", "ndf", "dtsx", "rdl", "dim"

***암호화 대상 경로**

"C:\\"
"C:\\Users\\[사용자 계정]\\Desktop"
"C:\\Users\\Public\\Desktop"
"C:\\Users\\[사용자 계정]\\Documents"
"C:\\Users\\[사용자 계정]\\Pictures"
"C:\\Users\\[사용자 계정]\\Desktop"
"C:\\Users\\[사용자 계정]\\Documents"
"C:\\Users\\[사용자 계정]\\Music"
"C:\\Users\\Public\\Music"
"C:\\Users\\Public\\Pictures"
"C:\\Users\\[사용자 계정]\\Videos"
"C:\\Users\\[사용자 계정]\\Downloads"

***암호화 제외 경로**

C:\\Windows
C:\\Windows\\system32
C:\\Windows\\SysWOW64
C:\\Program Files\\Common Files
C:\\Program Files (x86)\\Common Files
C:\\Program Files
C:\\Program Files (x86)

파일을 암호화하기 전, 아래의 서비스 종료 및 비활성화, 프로세스 종료 기능을 수행합니다. 이는 원활한 파일 암호화 기능을 수행하기 위한 것으로 보입니다.

***서비스 종료 대상 기능**

avpsus
McAfeeDLPAgentService
BMR Boot Service
NetBackup BMR MTFTP Service

***서비스 비활성화 대상**

SQLTELEMETRY
SQLTELEMETRY$ECWDB2
SQLWriter
SstpSvc

***프로세스 종료 대상 목록**

mspub.exe
mydesktopqos.exe
mydesktopservice.exe

또한 파일 암호화 진행시 쉐도우 볼륨 및 윈도 백업 관련 파일을 삭제하기 때문에 사용자 입장에서는 복호화키 없이는 파일을 원상복구하기 불가능해집니다.

*** 쉐도우 볼륨 삭제하는 명령어**

"Delete Shadows /all /quiet"
"resize shadowstorage /for=c: /on=c: /maxsize=401MB"
"resize shadowstorage /for=c: /on=c: /maxsize=unbounded"
"resize shadowstorage /for=d: /on=d: /maxsize=401MB"
"resize shadowstorage /for=d: /on=d: /maxsize=unbounded"
"resize shadowstorage /for=e: /on=e: /maxsize=401MB"
"resize shadowstorage /for=e: /on=e: /maxsize=unbounded"
"resize shadowstorage /for=f: /on=f: /maxsize=401MB"
"resize shadowstorage /for=f: /on=f: /maxsize=unbounded"
"resize shadowstorage /for=g: /on=g: /maxsize=401MB"
"resize shadowstorage /for=g: /on=g: /maxsize=unbounded"
"resize shadowstorage /for=h: /on=h: /maxsize=401MB"
"resize shadowstorage /for=h: /on=h: /maxsize=unbounded"
"Delete Shadows /all /quiet"

02 전문가 기고

일부 확장자(docx, pdf, xlsx, csv)의 경우 ftp 에 업로드하는 기능이 포함되어 있지만, 테스트 목적으로 보여집니다.

항목	값
FTP 도메인	ftp://files.000webhost.com/public_html/
ID	FTP UserName
PassWord	FTP Password

코로나 랜섬웨어는 이메일 첨부파일을 통해 초기 유포가 이뤄졌을 것으로 추정되며, 대다수의 랜섬웨어 공격이 악성 이메일을 통해 최초 공격이 시작되는 점을 염두에 두고 출처를 알 수 없거나 의심되는 메일에 대한 첨부파일 열람에 특히 주의를 기울여야 합니다.

이번 코로나 랜섬웨어의 경우 Hakbit 랜섬웨어의 변종이기 때문에, 기존에 이미 릴리즈되어 있는 Hakbit 랜섬웨어 복호화툴로는 대응이 가능할 지 확인해보았으나 복호화가 불가능함이 확인되었습니다. (2020/03/02 확인)

현재 알약에서는 해당 랜섬웨어에 대해 **Trojan.Ransom.Hakbit** 으로 탐지중입니다.

2. 기업 내부 보안 위협하는 '섀도우 IT', 어떻게 대응해야 할까?

업무 환경의 변화에 따라, 조직의 보안 관리자들은 개인의 디바이스 혹은 애플리케이션을 뜻하는 BYOD(Bring Your Own Device)와 BYOA(Bring Your Own Application), 그리고 Shadow IT(이하 섀도우 IT)로 인한 엔드포인트 보안 문제에 대해 고려하기 시작했습니다.

그래서 오늘은 엔드포인트 보안 전략 수립 시 기업들이 고려해야 할 사항과 필요한 솔루션에 대해 알아보려고 합니다.

섀도우 IT 로 사이버 위협에 노출되는 '엔드포인트'

다국적, 초국적 기업이 늘어나고 오피스 환경이 변화함에 따라 원격 근무를 활용하는 기업도 증가하고 있습니다.

포브스(Forbes)에 따르면, 미국의 경우 2007 년 대비 2019 년 원격 근무 비율이 159% 증가했으며, 영국은 인력의 50%가 원격 근무를 하는 것으로 추정됩니다. 이 같은 추세이다 보니, 업무용이 아닌 개인용 데스크톱이나 노트북을 회사의 업무에 사용하는 비율도 함께 증가하고 있습니다.

섀도우 IT 란 직원들이 IT 부서에서 승인받지 않은 클라우드 애플리케이션이나 서비스를 구입하고, 이를 IT 관리 부서나 책임자가 파악하지 못하는 현상을 일컫습니다.

IBM 이 1 천 곳의 기업을 대상으로 실시한 설문조사, 'Bring shadow IT into the light(2017)' 에 따르면, 기업들이 파악하지 못한 섀도우 IT 가 기업에서 파악하고 있는 클라우드 기반 애플리케이션(에버노트, 노션 등) 보다 10 배 가량 많은 것으로 나타났습니다.

다시 말해, 업무에 사용하는 디바이스와 애플리케이션 사용에 있어 효율과 편의성 등을 이유로 IT 보안 부서의 관리 범위를 벗어난 경우가 증가하고 있는 것입니다. 이러한 현상은 사이버 보안 위협 노출과 새로운 취약점의 등장 등 엔드포인트 보안 문제를 가져왔습니다.

조직들이 승인받지 않은 디바이스와 애플리케이션 사용에 따른 보안 관리 지점을 모두 파악하는 것은 사실상 불가능합니다. 따라서 보안 관리자가 파악하고 있는 전반적 가시성이 줄어들고, 내부에 악성코드가 발생했을 때 제대로 대응하기도 어려워지고 있는 것입니다.

뿐만 아니라 IT 관리 비용 또한 증가하고 있는데, 이는 기업의 IT 전략과 프로세스가 제대로 수립되지 않을 때의 손실과 IT 보안 관리 및 강화를 위한 비용이 추가로 발생하기 때문입니다.

틈새까지 완벽하게 엔드포인트를 지키는 방법은?

보안 관리자가 모든 직원의 IT 업무 환경을 제어하기는 어렵기 때문에, 관리 밖의 IT 서비스를 사용하면 임직원들이 본인도 모르는 사이, 랜섬웨어와 같은 보안 위협에 노출되는 상황은 꾸준히 발생할 것입니다. 그렇다면 우린 섀도우 IT 로 인한 보안 취약점을 어떻게 해결해야 할까요?

1. 패치 관리 솔루션

먼저, 패치 관리 솔루션을 통해서 엔드포인트의 하드웨어와 소프트웨어를 포함한 모든 인프라 가시성을 확보하고, 소프트웨어를 자동으로 패치하여 최신 버전 상태로 유지하는 방법이 있습니다. 하지만 관리 대상에 포함되지 않은 이벤트 등의 영역은 여전히 안전하지 않습니다.

2. 문서중앙화 솔루션

또한 엔드포인트 내 보관되어 있는 기업의 핵심 자산인 문서파일의 유출을 막는 문서중앙화 솔루션도 대안이 될 수 있습니다. 문서중앙화 솔루션은 개인 PC 내 문서 생산을 통제하기 때문에, 문서가 개인 계정의 클라우드 저장소나 이메일 등에 저장되는 것을 막을 수 있습니다.

하지만 문서중앙화는 구멍이 뚫린 엔드포인트를 보호하는 데에는 한계가 있습니다. 즉, 사이버 공격의 타깃이 되어도 공격자의 최종 목적지인 엔드포인트를 안전하게 보호할 수 있는 솔루션이 요구됩니다.

3. EDR

최근에는 안티바이러스의 보완재로 엔드포인트 위협 대응 솔루션(Endpoint Detection & Response, 이하 EDR) 개념이 국내 시장의 주목을 받고 있다. 단말에서 발생한 이벤트를 수집하여 위협을 가시화하고 알려지지 않은 위협을 찾아낼 수 있기 때문입니다.

EDR 은 예측-방어-탐지-대응 네 단계로 보안 영역을 나누어, 고도화된 위협을 면밀하게 대응하는 것이 특징입니다. 파일 정보만이 아니라 레지스트리, 프로세스, 네트워크 연결 정보 등을 수집하고 종합적인 분석을 통해 새로운 위협을 차단하거나 체계적인 사고 대응이 가능하기 때문에, 섀도우 IT 로 발생하는 보안 홀을 점검하고 관리할 수 있다는 기대를 받고 있습니다.

도입보다 운영이 중요한 EDR 솔루션

하지만 엔드포인트 보안의 새로운 대책으로 떠오른 EDR 을 향한 뜨거운 관심과 시장의 분위기는 다소 온도 차가 있습니다. EDR 은 도입도 도입이지만, 성공적인 운영이 관건이기 때문입니다. EDR 의 운용을 위해 관리자가 고려해야 할 필수 사항은 다음과 같습니다.

1. 한눈에 파악할 수 있는 위협 가시성 확보

IT 보안 관리자에게 가장 필요한 정보 중 하나는 시스템 내 위협의 전체적인 흐름 · 의심 위협의 종류 · 행위 · 공격 단계에 대한 정보와 이들 간의 연관 관계이므로, 이를 한눈에 파악할 수 있도록 엔드포인트 전체의 가시성을 확보하는 게 중요합니다.

이와 관련해 조직 내 엔드포인트 위협 정보 모니터링 시 커널 레벨의 동작 로그를 활용하는 EDR 솔루션을 선택하는 것도 방법이 될 수 있습니다.

이는 유저 레벨의 동작 로그 수집과 달리, 강력한 커널 레벨 로깅 기능으로 충돌 이슈, 로그 유실 및 서버 부하를 최소화해 조직 내 엔드포인트 위협 정보를 안정적으로 수집 · 제공할 수 있도록 합니다.

또한 엔드포인트 내 보관되어 있는 기업의 핵심 자산인 문서파일의 유출을 막는 문서중앙화 솔루션도 대안이 될 수 있습니다. 문서중앙화 솔루션은 개인 PC 내 문서 생산을 통제하기 때문에, 문서가 개인 계정의 클라우드 저장소나 이메일 등에 저장되는 것을 막을 수 있습니다.

하지만 문서중앙화는 구멍이 뚫린 엔드포인트를 보호하는 데에는 한계가 있습니다. 즉, 사이버 공격의 타깃이 되어도 공격자의 최종 목적지인 엔드포인트를 안전하게 보호할 수 있는 솔루션이 요구됩니다.

2. 운영 리소스 최소화 및 근본적인 대응을 위한 안티바이러스 연동

두 번째로 중요한 요소는 관리자의 리소스를 줄여주는 것입니다. 실제로 시장엔 많은 EDR 제품들이 출시돼 있지만, 사용자들이 선택에 어려움을 겪는 이유 중 하나는 과도한 의심 이벤트 알림으로 인한 보안 관리자의 업무부담 과중 문제가 해결되지 않는다는 점입니다.

EDR 은 기존 보안 솔루션이 탐지하지 못한 지능형 공격을 방어하기 위한 것으로, 보안 조직의 리소스가 추가로 투입되어야 하는 솔루션입니다. 하지만 알려진 악성코드의 악성행위의 경우 보안 관리자의 개입 없이도 EDR 솔루션에서 선차단-후보고하는 방식으로 운영된다면 절대적인 보안 알림의 수를 줄일 수 있습니다.

또한 EDR 에서 보안 담당자가 프로세스 격리, 차단 등 즉각적인 조치를 취하는 것은 임시 방책으로 볼 수 있으며, 최종적으로는 알려진 악성코드가 조직 내 운용 중인 안티바이러스에 반영되어 근본적인 치료와 대응이 가능해야 합니다.

따라서, 해당 EDR 솔루션이 안티바이러스와 유기적으로 연동이 되는지, 또는 동일한 보안 업체가 EDR 과 안티바이러스를 둘 다 제공해 단일 에이전트로 보다 손쉬운 관리가 가능한지 반드시 고려돼야 합니다.

3. 보안 전문성을 보완하는 표준 체계 형태의 위협 인텔리전스 제공

EDR 솔루션이 식별하지 못한 알려지지 않은 위협에 대해 근본적으로 대응하기 위해서는 행위 기반 탐지 정보를 해석할 수 있는 보안 전문성도 필수적 요소입니다.

보안을 위해선 전문 조직의 직접적 대응으로 놓칠 수 있는 엔드포인트 보안 영역에 대한 철저한 관리가 필요합니다. 하지만 국내 보안 환경 상 모든 조직에서 보안 전문가를 따로 두기란 사실상 불가능합니다.

따라서 보안 전문성을 보완할 수 있는 위협 인텔리전스를 제공하는지를 필수적으로 고려해야 합니다. 위협에 대한 식별 정보와 대응 가이드를 포함한 위협 인텔리전스는 보안 관리자의 의사 결정과 보안 정책 수립을 빠르게 도와, 신속한 엔드포인트 위협 대응을 가능케 합니다.

특히 타 솔루션의 정보를 함께 활용하여 위협 인텔리전스 시너지를 높이기 위해서는 위협 인텔리전스 공유 체계의 표준인 MITRE ATT&CK, STIX/TAXII 등이 지원되는 위협 인텔리전스가 필요합니다.

실제 조직 보안 환경이 고려된 EDR 솔루션 필요

EDR 솔루션을 조직 보안 환경에 안착시키기 위해서는 업무 환경에 맞는 운영 방식이 필요합니다. 구축 및 운영 리소스는 최소화하고, 엔드포인트 보안은 최대 효과를 낼 수 있는 솔루션이 요구됩니다.

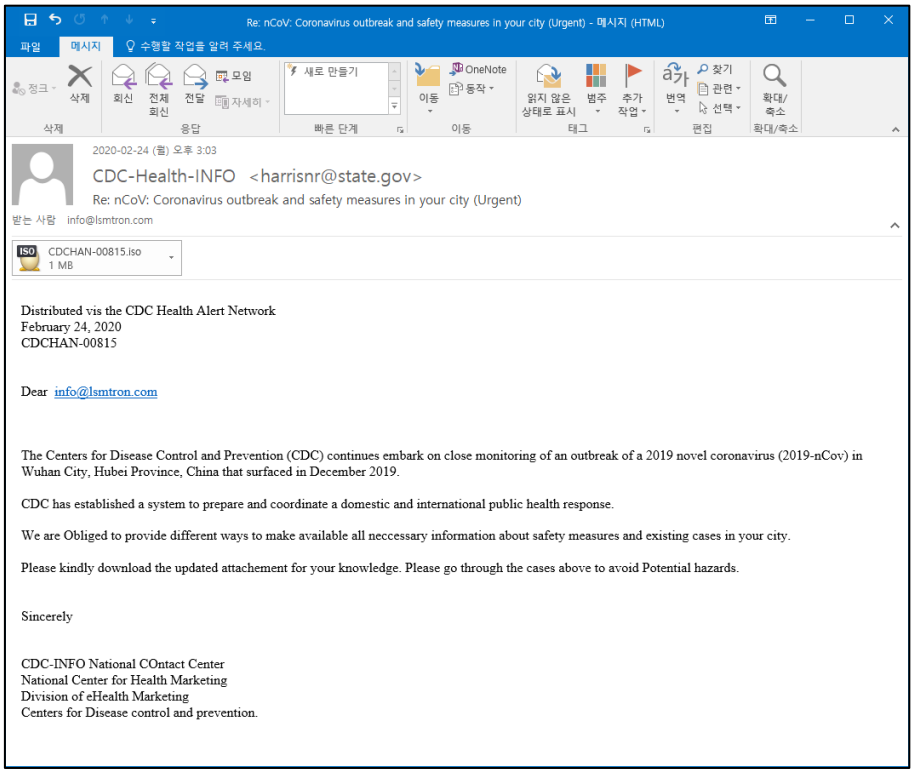
백신이나 EDR, 어느 하나의 솔루션만으로 진화하는 위협에 대응할 수 없습니다. 알려진 공격은 백신으로 차단하고, 알려지지 않은 공격은 행위기반 분석 기술을 탑재한 EDR 을 통해 탐지하며, 위협 인텔리전스와 비교해 빠르게 대응한 후, 솔루션이 판단하지 못한 고도화된 위협은 전문 조직이 직접 대응하면서 엔드포인트 보안 위협을 낮춰야 합니다. 다시 말하면, ▲알려진 공격을 선 차단할 수 있는 안티바이러스 연동 여부와 ▲알려지지 않은 위협에 대응할 수 있는 위협 인텔리전스의 결합 여부가 EDR 솔루션이 갖춰야할 필수적인 요소인 것입니다.

섀도우 IT 로 말미암은 보안홀로 발생하는 엔드포인트 위협에 실효적이고 빈틈없이 대응하기 위해, 실제 조직 보안 환경이 고려된 EDR 솔루션의 도입이 필요한 상황입니다.

03
악성코드 분석 보고

[Backdoor.Remcos.A] 악성코드 분석 보고서

최근 신종 코로나 바이러스의 확진자가 지속적으로 발생하면서, 국내뿐 아니라 해외에서도 신종 코로나바이러스에 대한 대중의 관심과 우려가 높아진 가운데 미국 질병통제예방센터(CDC)를 사칭하고 있는 이메일이 발견되었다. 파일명은 'CDCHAN-00815.iso'로 압축을 풀면 화면보호기 파일로 위장된 파일이 있고 실제로 악성 행위를 하는 실행 파일이다.



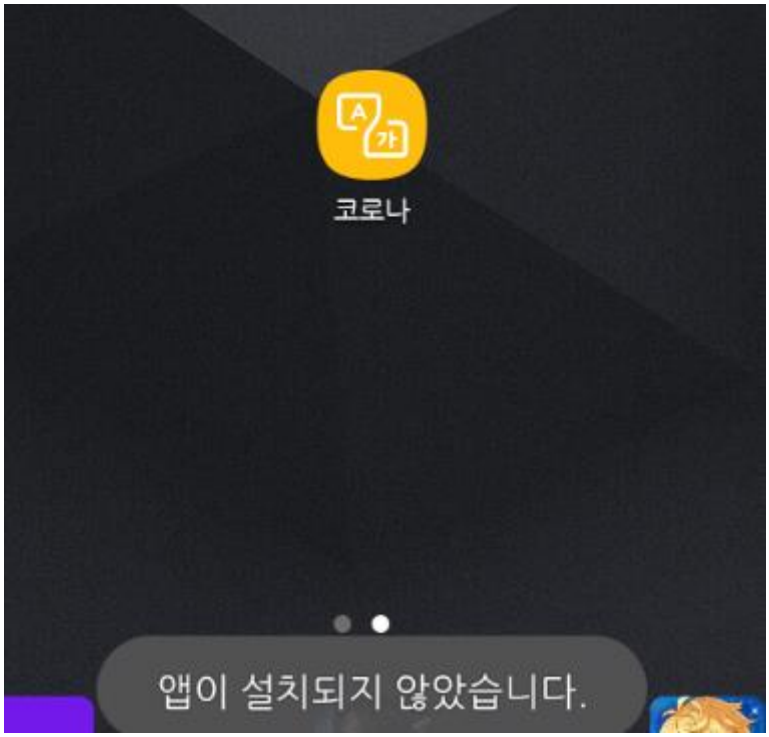
[그림] 수신된 이메일 화면

이번에 발견된 공격의 특징은 해외 업체에서 윈도우를 관리하기 위해 개발된 'Remcos' 프로그램을 공격자들이 원격 접근 툴로 악용한다는 점이다. 위와 같은 악성코드 피해를 예방하기 위해서는 출처가 불분명한 곳에서의 URL 클릭 혹은 파일 다운로드를 지양해야 한다.

현재 알약에서는 해당 악성 코드를 'Backdoor.Remcos.A' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Spyware.Android.Agent] 악성코드 분석 보고서

해당 악성 앱은 "코로나"라는 한글 앱 명을 사용하며 위치 및 카메라 관련 파일을 탈취하고 원격명령을 통해서 추가 악성 행위를 한다. 특히, 앱의 이름과 수정 날짜를 보면 현재 이슈인 코로나를 이용하여 악성 행위를 하고자 했음을 알 수 있다.



DOSTIME frFileTime	16:29:32
DOSDATE frFileDate	02/27/2020

[그림] 바로 숨겨지는 아이콘과 앱의 수정 날짜

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

04

글로벌 보안 동향

Mailto (NetWalker) 랜섬웨어, 기업 네트워크 노리기 시작

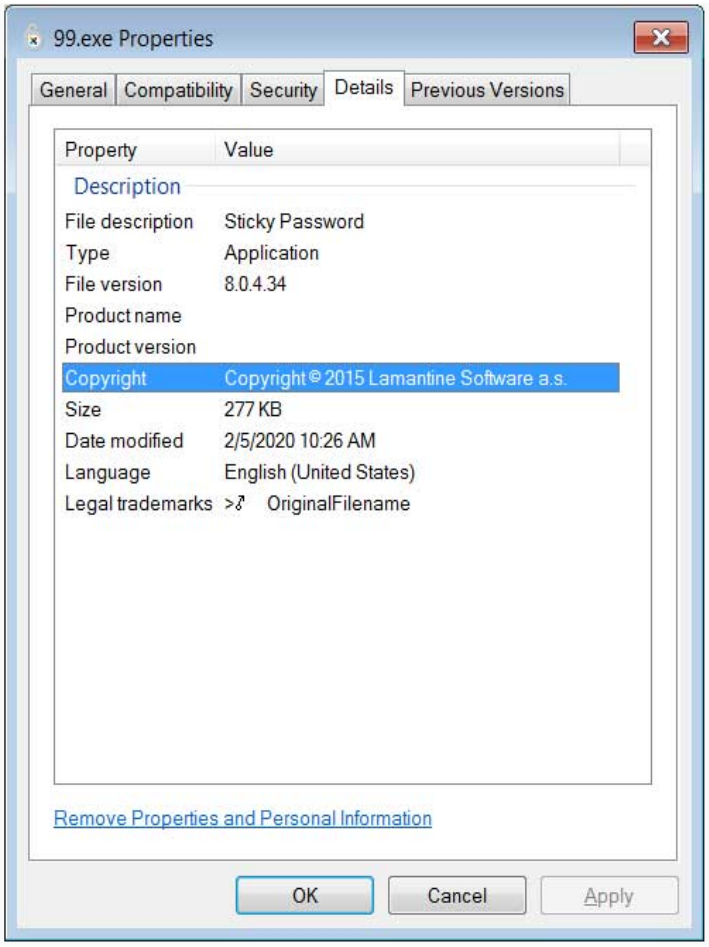
Mailto (NetWalker) Ransomware Targets Enterprise Networks

Mailto 또는 Netwalker 라 알려진 랜섬웨어가 기업 네트워크를 해킹하여 연결된 모든 윈도우 기기를 암호화하기 시작한 것으로 나타났다. 2019 년 8 월, ID Ransomware 에서 Mailto 라는 새로운 랜섬웨어가 발견되었다. 이 랜섬웨어의 이름은 암호화된 파일의 확장자에서 따왔다.

금일 호주의 Toll Group 이 회사의 네트워크가 Mailto 랜섬웨어의 공격을 받았다고 발표하여 이 랜섬웨어가 기업을 노린다는 사실이 처음 밝혀졌다. 이 랜섬웨어는 사용하는 확장자에서 따온 이름인 Mailto 라 불리고 있지만, 복호화 툴 중 하나를 분석 결과 Netwalker 라는 이름을 사용하고 있었던 것으로 밝혀졌다.

Mailto / Netwalker 랜섬웨어

MalwareHunterTeam 에서 BleepingComputer 에 공유한 Mailto 랜섬웨어의 최근 샘플의 실행 파일은 'Sticky Password' 소프트웨어로 위장하려 시도했다.



[그림 1] Sticky Password 로 위장한 실행 파일

이 랜섬웨어는 실행된 후 랜섬노트 템플릿, 랜섬노트 파일명, ID, 확장자의 길이, 화이트리스팅된 파일, 폴더, 확장자 등 기타 구성 옵션이 포함된 내장된 구성 파일을 사용한다. 이 랜섬웨어를 분석한 SentinelLabs의 Vitali Kremez는 이 구성 파일이 다른 랜섬웨어에 비해 매우 정교하고 상세하게 작성되었다고 밝혔다. 이 샘플 내장된 구성 파일은 여기에서 살펴볼 수 있다.


```
{
 "mpk :"EXgCIpycIJzspm07Loi9L5uOcxC+VZ/NjxWfOn7UqVE=",
 "mode :0,
 "thr :1500,
 "spsz :16384,
 "namesz :6,
 "idsz :5,
 "crmask :".mailto[{mail1}].{id}",
 "mail :["sevenoneone@cock.li" ,"kavariusing@tutanota.com"],
 "lfile :"{ID}-Readme.txt",
 "lend
 :"SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQuDQpBbGwgZW5jcnlwdGVkIGZpbGVzIGZvciB0aGlzIGNvbXB1dGVyIGhhcyBleHRlb
 nNpb246IC57aWR9DQoNCi0tDQoNCklmIGZvciBzb21lIHJlYXNvbiB5b3UgcmVhZCB0aGlzIHRleHQgYmVmb3JlIHRoZSBlbmNyeXB0aW9u
 IGVuZGVkLA0KdGhpcyBjYW4gYmUgdW5kZXJzdG9vZCBieSB0aGUgZmFjdCB0aGF0IHRoZSBjb21wdXRlciBzbG93cyBkb3duLCANCmFuZCB
 5b3VyIGhlYXJ0IHJhdGUgaGFzIGluY3JlYXNlZCBkdWUgdG8gdGhlIGFiaWxpdHkgdG8gdHVybiBpdCBvZmYsDQp0aGVuIHdlIHJlY29tbW
 VuZCB0aGF0IHlvdSBtb3ZlIGF3YXkgZnJvbSB0aGUgY29tcHV0ZXIgYW5kIGFjY2VwdCB0aGF0IHlvdSBoYXZlIGJlZW4gY29tcHJvbWlzZ
 WQsDQpyZWJvb3Rpbmcvc2h1dGRvd24gd2lsbCBjYXVzZSB5b3UgdG8gbG9zZSBmaWxlcyB3aXRob3V0IHRoZSBwb3NzaWJpbGl0eSBvZiBy
 ZWNvdmVyeSBhbmQgZXZlbiBnb2Qgd2lsbCBub3QgYmUgYWJsZSB0byBoZWxwIHlvdSwNCml0IGNvdWxkIGJlIGZpbGVzIG9uIHRoZSBuZXR
 3b3JrIGJlbG9uZ2luZyB0byBvdGhlciBlc2Vycywgc3VyZSB5b3Ugd2FudCB0byB0YWtlIHRoYXQgcmVzcG9uc2liaWxpdHk/DQoNCi0tDQ
 oNCk91ciBlbmNyeXB0aW9uIGFsZ29yaXRobXMgYXJlIHZlcnkgc3Ryb25nIGFuZCB5b3VyIGZpbGVzIGFyZSB2ZXJ5IHdlbGwgcHJvdGVjd
 GVkLCB5b3UgY2FuJ3QgaG9wZSB0byByZWNvdmVyIHRoZW0gd2l0aG91dCBvdXIgaGVscC4NClRoZSBvbmx5IHdheSB0byBnZXQgeW91ciBm
 aWxlcyBiYWNrIGlzIHRvIGNvb3BlcmF0ZSB3aXRoIHVzIGFuZCBnZXQgdGhlIGRlY3J5cHRlciBwcm9ncmFtLg0KRG8gbm90IHRyeSB0byB
 yZWNvdmVyIHlvdXIgZmlsZXMgd2l0aG91dCBhIGRlY3J5cHQgcHJvZ3JhbSwgeW91IG1heSBkYW1hZ2UgdGhlbSBhbmQgdGhlbiB0aGV5IH
 dpbGwgYmUgaW1wb3NzaWJsZSB0byByZWNvdmVyLg0KDQpXZSBhZHZpc2UgeW91IHRvIGNvbnRhY3QgdXMgYXMgc29vbiBhcyBwb3NzaWJsZ
 Swgb3RoZXJ3aXNlIHRoZXJlIGlzIGEgcG9zc2liaWxpdHkgdGhhdCB5b3VyIGZpbGVzIHdpbGwgbmV2ZXIgYmUgcmV0dXJuZWQuDQpGb3Ig
 dXMgdGhpcyBpcyBqdXN0IGJ1c2luZXNzIGFuZCB0byBwcm92ZSB0byB5b3Ugb3VyIHNlcmlvdXNuZXNzLCB3ZSB3aWxsIGRlY3J5cHQgeW9
 1IHNvbWUgZmlsZXMgZm9yIGZyZWUsIA0KYnV0IHdlIHdpbGwgbm90IHdhaXQgZm9yIHlvdXIgbGV0dGVyIGZvciBhIGxvbmcgdGltZSwgbW
 FpbCBjYW4gYmUgYWJ1c2VkLCB3ZSBhcmUgbW92aW5nIG9uLCBodXJyeSB1cCB3aXRoIHRoZSBkZWNpc2lvbi4NCg0K0KFvbnRhY3QgdXM6D
 QoxLnttYWlsMX0NCjIue21haWwyfQ0KDQpEb24ndCBmb3JnZXQgdG8gaW5jbHVkZSB5b3VyIGNvZGUgaW4gdGhlIGVtYWlsOg0Ke2NvZGV9
 ",
 "white :{
    "path :["*system volume
    information","*windows.old","*:\users\*\*temp","*msocache","*:\winnt","*$windows.~ws","*perflogs","*boot
    ","*:\windows","*:\program file*","\vmware","\\*\users\*\*temp","\\*\winnt
    nt","\\*\windows","*\program
    file*\vmwaree","*appdata*microsoft","*appdata*packages","*microsoft\provisioning","*dvd
    maker","*Internet Explorer","*Mozilla","*Old Firefox data","*\program file*\windows media*","*\program
    file*\windows portable*","*windows defender","*\program file*\windows nt","*\program file*\windows
```

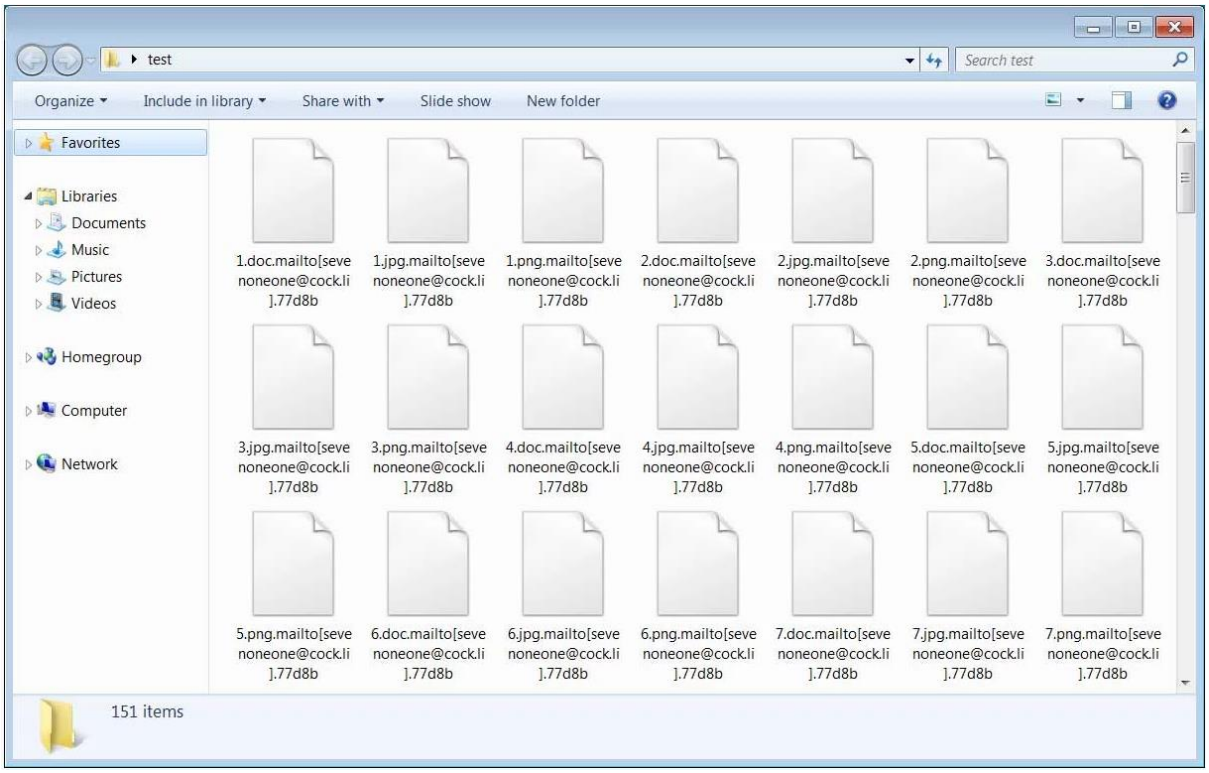

[그림 2] 랜섬웨어 구성 파일

랜섬웨어 대부분은 암호화를 제외할 폴더, 파일, 확장자를 화이트리스트를 통해 관리한다. Mailto 는 다른 랜섬웨어와 비교했을 때 엄청나게 긴 화이트리스트를 사용한다. 그 예로, 암호화를 제외하는 폴더 목록은 아래와 같다.

```
*system volume information
*windows.old
*:\users\*\*temp
*msocache
*:\winnt
*$windows.~ws
*perflogs
*boot
*:\windows
*:\program file*
\vmware
\\*\users\*\*temp
```

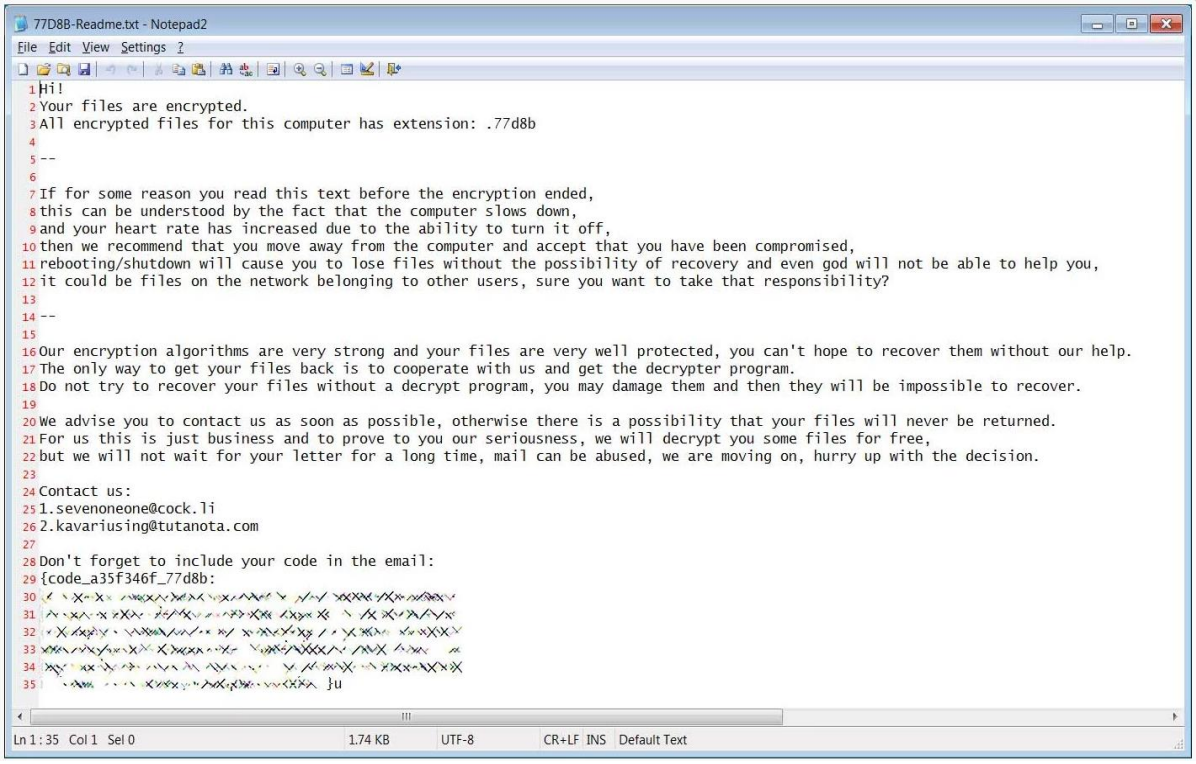
```
\\*\winnt nt
\\*\windows
*\program file*\vmwaree
*appdata*microsoft
*appdata*packages
*microsoft\provisioning
*dvd maker
*Internet Explorer
*Mozilla
*Old Firefox data
*\program file*\windows media*
*\program file*\windows portable*
*windows defender
*\program file*\windows nt
*\program file*\windows photo*
*\program file*\windows side*
*\program file*\windowspowershell
*\program file*\cuas*
*\program file*\microsoft games
*\program file*\common files\system em
*\program file*\common files\*shared
*\program file*\common files\reference ass*
*\windows\cache*
*temporary internet*
*media player
*:\users\*\appdata\*\microsoft
\\*\users\*\appdata\*\microsoft
```

Mailto 랜섬웨어는 파일을 암호화한 후 .mailto[{mail1}].{id}와 같은 형태로 파일명을 변경한다. 예를 들면, 1.doc 파일이 암호화될 경우 1.doc.mailto[sevenoneone@cock.li].77d8b 와 같은 형태로 파일명이 변경된다.



[그림 3] 암호화된 파일

또한 랜섬웨어는 파일 이름이 {ID}-Readme.txt 인 랜섬노트를 생성한다. 연구원들이 실행한 한 테스트에서는 랜섬노트의 이름이 77D8B-Readme.txt 로 생성되었다.



[그림 4] Mailto / Netwalker 랜섬노트

이 랜섬웨어에 대한 분석은 아직 진행 중이며, 무료 복호화 툴을 만들 수 있을지 여부는 알려지지 않은 상태이다.

이 랜섬웨어의 이름은 Mailto 인가, 아니면 Netwalker 인가?

보통 새로운 랜섬웨어가 발견되면 발견자나 연구원들이 랜섬웨어 개발자가 붙인 이름에 대한 표시를 찾는다. 이러한 표시를 찾을 수 없을 경우, 대부분 이 랜섬웨어가 사용하는 확장자를 따 이름을 짓는다. Mailto 랜섬웨어에는 이름에 대한 표시가 없었기 때문에 확장자에서 이름을 따와 사용하고 있었다. 하지만 얼마 후 Covewave 가 이 랜섬웨어의 복호화 툴을 발견 후 확인 결과 개발자가 이 랜섬웨어에 붙인 이름이 'Netwalker'였음이 밝혀졌다.

[그림 5] Netwalker 복호화 툴

따라서 이 랜섬웨어의 실제 이름은 Netwalker 가 맞지만, 이미 Mailto 로 알려져 있기 때문에 혼동을 줄이기 위해 기존 이름을 사용하는 경우가 많다.

[출처] https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/

인터넷에 연결된 의료 장비 중 약 절반 BlueKeep 에 취약해

Cybersecurity warning: Almost half of connected medical devices are vulnerable to hackers exploiting BlueKeep

인터넷에 연결된 의료 장비들이 또다시 BlueKeep 에 취약한 것으로 나타나 환자와 병원 직원들이 사이버 공격을 받을 위기에 처했다. BlueKeep 은 작년 발견된 마이크로소프트의 원격 데스크톱 프로토콜 (RDP) 서비스의 취약점으로 Windows 7, Windows Server 2008 R2, Windows Server 2008 에 영향을 준다. 마이크로소프트는 2019 년 5 월 BlueKeep 에 대한 패치를 발행했으며, 미국 NSA 와 영국 NCSC 를 포함한 보안 당국도 취약한 시스템을 패치할 것을 권고하는 긴급 경고를 발행했다. BlueKeep 은 WannaCry 를 퍼뜨리는데 일조한 EternalBlue 와 유사한 방식으로 웜처럼 배포될 수 있을 것이라는 우려가 있었다. 하지만 반복적인 경고에도 불구하고 많은 윈도우 시스템들과 맞춤형 의료 기기들은 BlueKeep 에 취약한 채 방치되고 있었다.

의료계 사이버 보안 회사인 CyberMDX 에 따르면, 일반 병원 내 윈도우 기기들 중 22%가 패치를 하지 않아 BlueKeep 에 노출되어 있는 것으로 나타났다. 윈도우에서 실행되는 인터넷 연결 의료기기의 경우 노출된 기기의 수는 45%로 약 절반가량이 취약한 것으로 드러났다. 병원 네트워크에 연결된 기기에는 방사선 장비, 모니터, 엑스레이, 초음파기기, 마취 기계 등이 있다. 이러한 기기가 패치되지 않았을 경우, 병원 네트워크와 환자들이 BlueKeep 을 노리는 해커들의 공격에 피해를 입을 수 있다. 하지만 병원에서는 지속적으로 환자를 관리해야 하기 때문에 업데이트를 위해 기기를 끌 시간이 부족해 패치가 어려운 상황이다. 또한 병원 네트워크의 규모는 너무나도 거대해 IT 부서에서 패치를 누락하는 경우가 발생할 수 있다.

병원에서 발생하는 주요 문제 중 하나는 지원이 중단된 소프트웨어를 사용한다는 점이다. 예를 들면, 병원 네트워크에서는 BlueKeep 에 취약하고 마이크로소프트에서 더 이상 지원하지 않는 윈도우 7 을 아직까지 흔히 사용하고 있다. 병원 네트워크 내 구형 시스템에서 의료기기를 계속 운영해야 할 상황일 경우, 이 기기를 나머지 네트워크에서 분리하거나 외부 인터넷 연결을 차단할 것을 권장했다. Geffen 은 "NAC 솔루션이나 내부 방화벽을 통해 네트워크나 VLAN 의 불필요한 포트로 들어오는 트래픽을 차단하는 것이 도움이 될 수 있다." 라고 밝혔다. 하지만 가장 중요한 것은 BlueKeep 취약점에 대한 패치를 가능한 한 빨리 적용하는 것이다. 최신 보안 업데이트를 적용은 해킹 사고를 가장 확실하게 예방하는 방법이다..

[출처]https://www.zdnet.com/article/cybersecurity-warning-almost-half-of-connected-medical-devices-are-vulnerable-to-hackers-exploiting-bluekeep/

구글 인증 2FA 코드를 탈취 가능한 안드로이드 악성코드 발견

Android malware can steal Google Authenticator 2FA codes

보안 연구원들이 '구글 인증기' 를 통해 생성된 OTP 를 추출하여 탈취할 수 있는 안드로이드 악성코드 변종을 발견했다고 밝혔다. 구글 인증기는 많은 온라인 계정이 이중 인증(2FA) 시 사용하는 모바일 앱이다.

구글은 지난 2010 년 이 모바일 인증 앱을 출시했다. 이 앱은 사용자가 온라인 계정에 로그인할 때 로그인 창에 입력해야 하는 6~8 자리 코드를 생성하여 작동한다. 구글은 SMS 기반 OTP 에 대한 대안으로 이 인증기를 출시했다. 구글 인증기 코드는 사용자의 스마트폰에서 생성되고 안전하지 않은 모바일 네트워크를 통해 이동하지 않기 때문에 SMS 기반 인증 방식보다 안전한 것으로 간주되고 있다.

CERBERUS, 인증기의 OTP 탈취 기능 추가해

ThreatFabric 의 보안 연구원들은 보고서를 발표해 인증기의 OTP 를 훔치는 기능을 포함하는 Cerberus 샘플을 발견했다고 밝혔다. Cerberus 는 2019 년 6 월 새로이 출시된 안드로이드 뱅킹 트로이목마다. 이 트로이목마는 접근성 권한을 악용하여 구글 인증기 애플리케이션에서 2FA 코드를 훔칠 수 있다. 또한 인증기 앱이 실행 중일 경우, 해당 앱 인터페이스의 내용을 받아와 C&C 서버로 전송할 수 있다. ThreatFabric 은 이 새로운 기능이 현재 온라인 해킹 포럼에 광고 및 판매되는 Cerberus 의 버전에서는 활성화가 되어 있지 않다고 밝혔다. 그리고 발견된 Cerberus 변종은 아직 테스트 단계인 것으로 추측되며, 빠른 시일 내에 공개될 수 있을 것으로 보인다고 전했다.

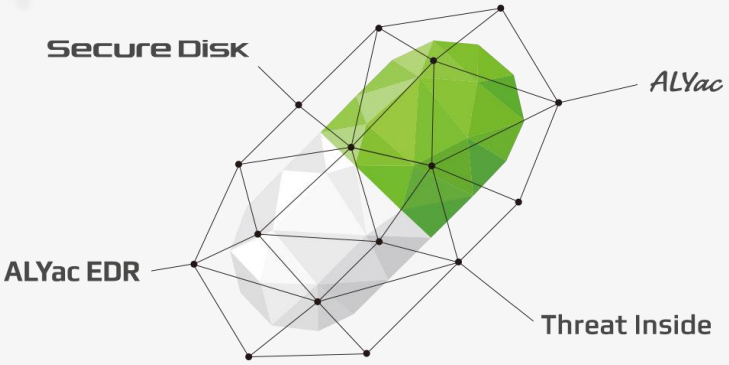
은행 계정에서 이중 인증을 우회하기 위해 새로운 기능 개발한 것으로 보여

연구원들은 Cerberus 뱅킹 트로이목마가 가장 상위 클래스 악성코드인 원격 접속 트로이목마(RAT)에서 일반적으로 찾아볼 수 있는 것과 동일한 기능을 포함하고 있어 매우 우수한 편이라고 밝혔다. Cerberus 운영자는 이 RAT 기능을 통해 원격으로 감염된 기기에 연결하여 기기 소유자의 뱅킹 크리덴셜을 사용해 온라인 뱅킹에 로그인하고, 이중 인증이 설정되어 있을 경우 인증기 OTP 탈취 기능을 통해 이중 인증을 우회할 수 있게 된다. 연구원들은 Cerberus 트로이목마가 온라인 뱅킹 계정 관련 이중 인증 필요시 이 기능을 사용할 것으로 추측했지만, 이메일 받은 편지함, 코드 저장소, 소셜 미디어 계정, 인트라넷 등에서 이중 인증이 걸린 다른 계정에 이를 악용할 수 있을 가능성도 있다고 밝혔다.

지금까지는 극히 적은 해커 그룹과 악성코드 변종만이 다중 인증 솔루션을 우회할 수 있었다. 만약 이 기능이 의도한 대로 작동하고 Cerberus 와 함께 배포될 경우 이 트로이목마는 악성코드 계의 엘리트로 급부상할 것이다. Cerberus 에 대한 자세한 내용은 ThreatFabric 의 보고서에서 확인할 수 있다.

[출처] https://www.zdnet.com/article/android-malware-can-steal-google-authenticator-2fa-codes/

https://www.threatfabric.com/blogs/2020_year_of_the_rat.



(주)이스트시큐리티

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