ESTSECURITY

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

악성코드 분석 리포트

by 알약(Alyac) · 2018. 9. 20. 14:58

0

ESTSECURITY

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.

ESTSECURITY

ESTSECURITY

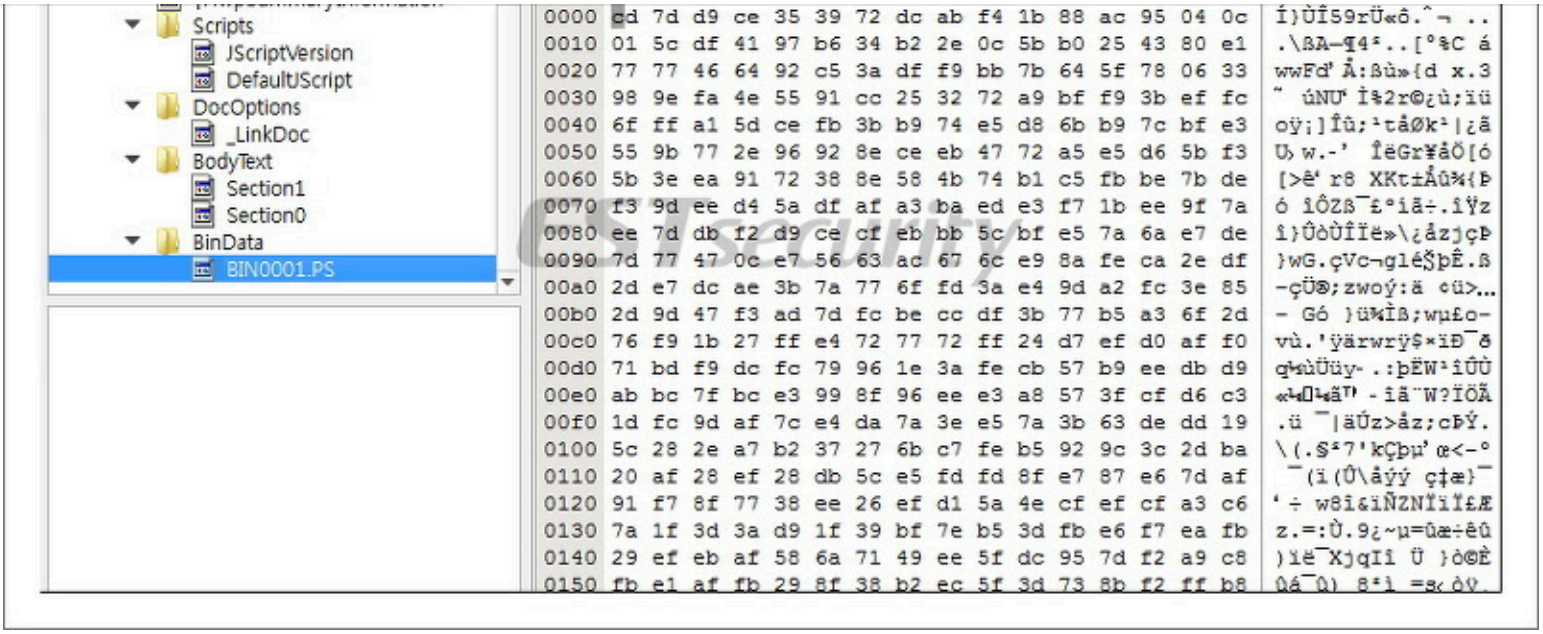
[201809]_Operation Ghost Puppet_Intelligence Report.pdf

먼저 'Ghost Puppet(유령 꼭두각시)'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.

[그림 3] 포스트스크립트에 포함된 쉘코드

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

ESTSECURITY

[그림 4] 다운로더 코드

운영체제 비트	페이로드 다운로드 C&C
32비트	https://tpddata[.]com/flash/gcoin2[.]swf
64비트	https://tpddata[.]com/flash/gcoin4[.]swf

[표 1] 페이로드 다운로드 C&C 목록

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

ESTSECURITY

[그림 5] C&C 연결 코드

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

[표 2] 악성코드에서 사용하는 C&C 정보

C&C에서 명령을 받은 경우, 공격자가 전송한 명령어에 따라 악성 기능이 수행된다. 원격 제어 코드 및 명령어에 따른 기능을 정리한 표는 다음과 같습니다.

[그림 6] 원격 제어 코드

다음은 명령어 및 기능을 설명한 표 입니다.

명령어	기능 설명
0x1827	OS 버전, 컴퓨터 이름 등 감염 기기 정보 전송
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

ESTSECURITY

0x183C	웹 서버로부터 데이터 다운 및 C&C 업로드

[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(1416424660925.hwp)(정상

[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.

ESTsecurity

파일 이름			저장한 작성자		저장 시
현종석 트레이딩시스템 경력기술서.hwp	-	user-pc	TATIANA	2017.10.04 15:20:00	2018.04. 11:05:4
거래처 원장.hwp	거래처 원장	TATIANA	TATIANA	2018.04.10 03:00:59	2018.04. 03:18:3
10년안에 대세가 될 기술 21가지.hwp	10년 안에 대세가 될 기술 21가지	Grumpy	TATIANA	2017.11.22 02:28:05	2018.05. 00:21:4
국방부 프라이버시 정보보호.hwp	붙임2	Lee Changhun	TATIANA	2018.04.23 01:40:58	2018.05. 00:23:0
김정민_포폴.hwp	김정민	alosha	User	2017.11.02 02:52:03	2018.05. 01:41:2
죽음에 대한 이해와 성찰.hwp	죽음에 대한 이해와 성찰	jae	TATIANA	2018.06.01 01:53:51	2018.06. 01:54:0
미국의 대테러전쟁.hwp	미국의 대테러전쟁	-	TATIANA	2018.06.01 01:54:18	2018.06. 01:54:3
나의 참전수기 모음.hwp	피묻은 나의 6.25전쟁수기	-	TATIANA	2006.05.15 09:03:25	2018.06. 01:55:0
신재영 전산담당 경력.hwp	표준 이력서	비즈폼 (bizforms.co.kr)	TATIANA	2017.03.21 04:30:05	2018.06. 00:49:3
금융안정 컨퍼런스 개최결과.hwp	인 사 발 령(안)	-	Mosf	2017.11.07 01:39:32	2018.06. 10:01:1
2018년 운세.hwp	-	Windows User	TATIANA	2018.04.18 15:05:00	2018.06. 01:24:4
백서v1.0[447].hwp	WRITTEN BY	User	User	2018.07.27 03:21:00	2018.07. 04:41:5
2018 대한민국 대중문화예술상[440].hwp	-	-	이현주	2009.05.12 09:16:04	2018.07. 01:06:1

ESTSECURITY

일일동향보고_180913.hwp	2014	상호	USER	2014.06.26 23:06:06	2018.09 23:51:0

[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 주제
4월	현종석 트레이딩시스템 경력기술서.hwp	이력서
	거래처 원장.hwp	회사 외상 매출 장부
5월	10년안에 대세가 될 기술 21가지.hwp	미래의 IT 기술 설명
	국방부 프라이버시 정보보호.hwp	국방부 정보보호 규정 설명
	김정민_포폴.hwp	이력서 및 포트폴리오
6월	죽음에 대한 이해와 성찰.hwp	'죽음에 대한 이해와 성찰의 요청' 논문
	미국의 대테러전쟁.hwp	'미국의 대테러전쟁' 연구논문
	나의 참전수기 모음.hwp	6.25 전쟁 및 베트남전 참전수기
	신재영 전산담당 경력.hwp	이력서
	금융안정 컨퍼런스 개최결과.hwp	'「2018 G20 글로벌 금융안정 컨퍼런스」 개최 결 보도자료
	2018년 운세.hwp	2018년 양띠 운세 관련 내용
7월	백서v1.0[447].hwp	가상화폐 거래소 설명
	2018 대한민국 대중문화예술상[440].hwp	2018년 대중문화예술상 후보
8월	유사수신행위 위반통보.hwp	유사수신행위 관련 위반 통보
9월	일일동향보고_180913.hwp	부동산 관련 일일 동향

[표 5] 시기별 각 악성 한글 문서 별 본문 내용

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.

ESTsecurity

력기술서.hwp	11:05:42	1Byte XOR 고정키 사용	고정키(0x29)
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		
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	1Byte XOR 고정키 + 가변키(0x00 ~ 0xFF) 사용	고정키(0x29) + 가변키(0x00 ~ 0xFF)
금융안정 컨퍼런스 개최결과.hwp	2018.06.14 10:01:17		
국제금융체제 실무그룹 회의결과.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	16Byte XOR 고정키 사용	0x1F1D3EB92305EDC2098CEB4931 3A59
2018 대한민국 대중문화예술상[440].hwp	2018.07.31 01:06:17		0xB95180B9AF1C59CAEF465A84C3 BAD8
유사수신행위 위반통보.hwp	2018.08.06 02:31:22		0xC9582680978FDE80593F2BC164 AC6F
일일동향보고_180913.hwp	2018.09.12 23:51:06		0x4EA3B485752D60E75F7F72D372F 2E4

ESTSECURITY

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.

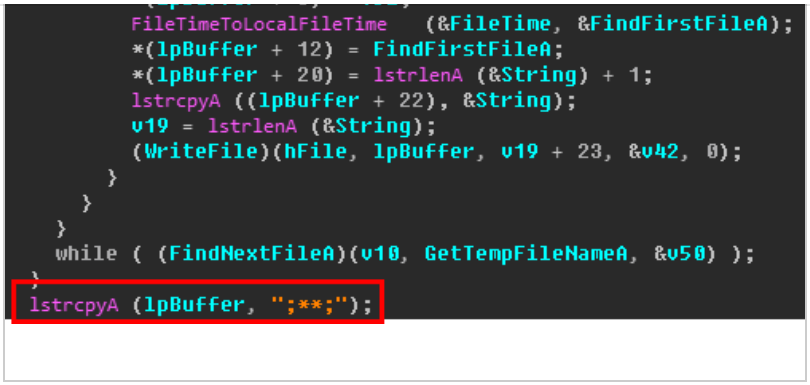
2009년 7월 7일 7.7 디도스 사건	2012년 6월 9일 중앙일보 해킹 사건
A7328FB36AF985BCAE0ED4EC7FA75659	78E8C150481107D7A5ED99E7E420FD24

```
      if ( FindFileData.dwFileAttributes & 0x10 )
        strncpy(&v2[v3], ":RV:", 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);
```

```
      if ( FindFileData.dwFileAttributes & 0x10 )
        v2(&Dest, ":DR:|");
      else
        v2(&Dest, ":FL:|");
      v4 = strlen(FindFileData.cFileName) + 1;
      v2(&Dest, FindFileData.cFileName);
      v2(&Dest, word_10006058);
      sprintf(v1, "%d|", FindFileData.nFileSizeLow
      v5 = strlen(v1) + 1;
      v2(&Dest, v1);
      sprintf(v1, "%d|", FindFileData.nFileSizeHig
      v6 = strlen(v1) + 1;
      v2(&Dest, v1);
      sprintf(v1, "%d|", FindFileData.ftLastWriteT
      v3 += v4 - 1 + 6 + v5 - 1 + 1 + v6 - 1 + 1 +
      v2(&Dest, v1);
    }
  }
  while ( FindNextFileA(hFindFile, &FindFileData)
}
if ( v3 )
  v2(&Dest, "<;;<");
else
  lstrcpyA(&Dest, "<;;<");
```

Ghost Puppet(gcoin2.swf)
A7C804B62AE93D708478949F498342F9

ESTSECURITY



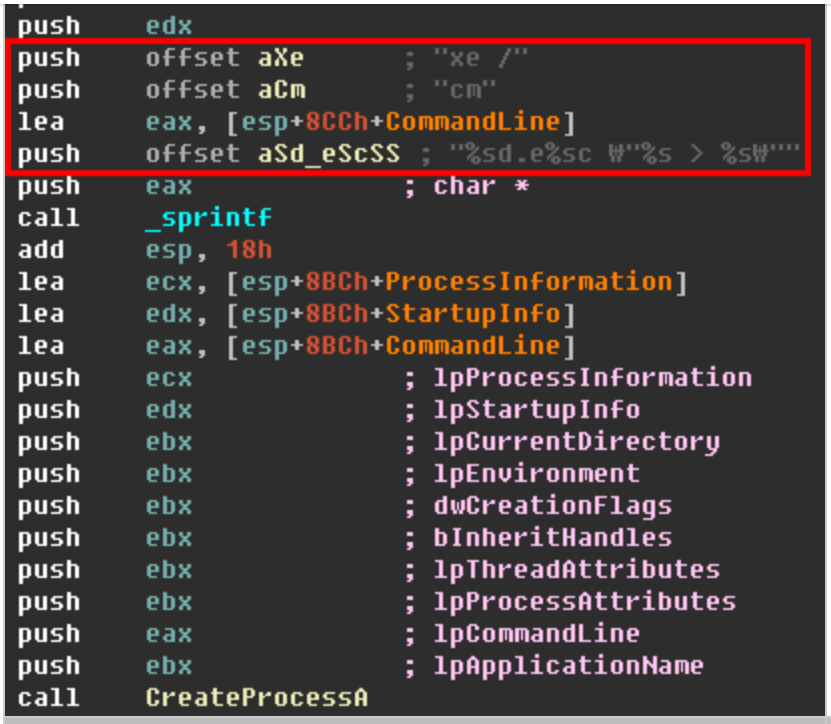
[그림 9] 각 사건 악성코드에서 확인되는 수집 시그니처 문자열

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 명령 프롬프트에서 명령어 수행 결과를 파일로 출력하는 기능을 하며, ‘2>&1’는 명령어 실행에 따른 에러 메시지를 파일로 출력합니다.

2009년 7월 7일 7.7 디도스 사건	2011년 04월 12일 농협 해킹 사건
A7328FB36AF985BCAE0ED4EC7FA75659	7706D38718707A73DCE032F79EEA43E

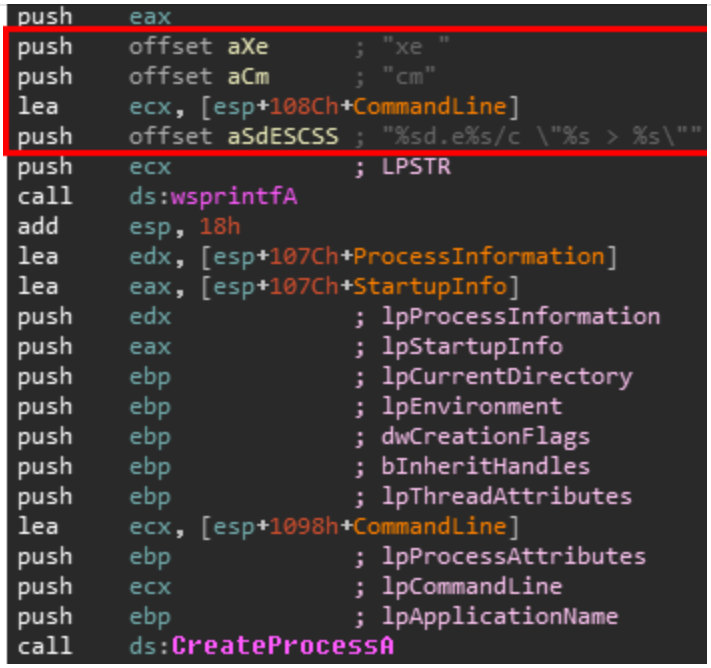
ESTSECURITY



```
push    edx
push    offset aXe      ; "xe /"
push    offset aCm      ; "cm"
lea     eax, [esp+8CCh+CommandLine]
push    offset aSd_eScSS ; "%sd.e%sc W"%s > %sW""
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

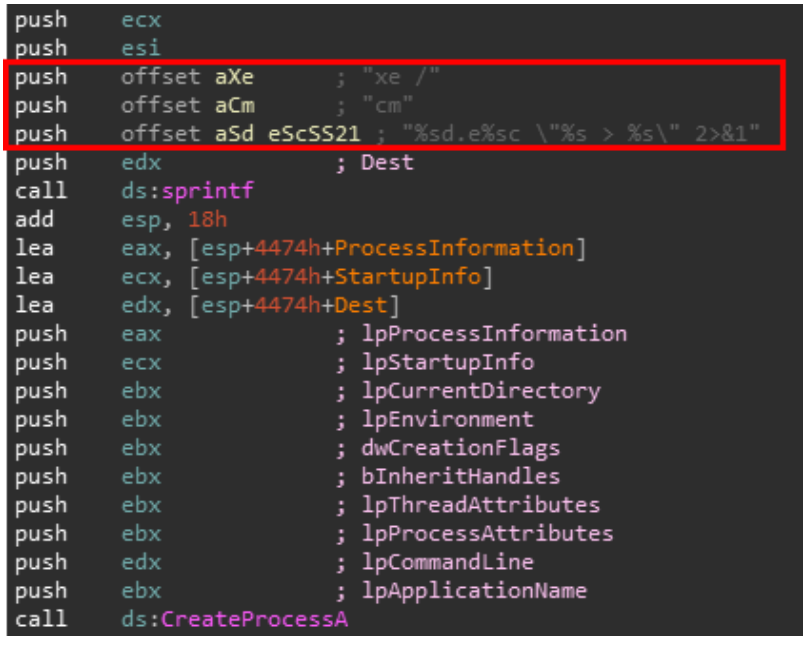
78E8C150481107D7A5ED99E7E420FD24



```
push    eax
push    offset aXe      ; "xe "
push    offset aCm      ; "cm"
lea     ecx, [esp+108Ch+CommandLine]
push    offset aSdESCSS ; "%sd.e%s/c \"%s > %s\""
push    ecx             ; LPSTR
call    ds:wsprintfA
add     esp, 18h
lea     edx, [esp+107Ch+ProcessInformation]
lea     eax, [esp+107Ch+StartupInfo]
push    edx             ; lpProcessInformation
push    eax             ; lpStartupInfo
push    ebp             ; lpCurrentDirectory
push    ebp             ; lpEnvironment
push    ebp             ; dwCreationFlags
push    ebp             ; bInheritHandles
push    ebp             ; lpThreadAttributes
lea     ecx, [esp+1098h+CommandLine]
push    ebp             ; lpProcessAttributes
push    ecx             ; lpCommandLine
push    ebp             ; lpApplicationName
call    ds:CreateProcessA
```

2013년 06월 25일 청와대

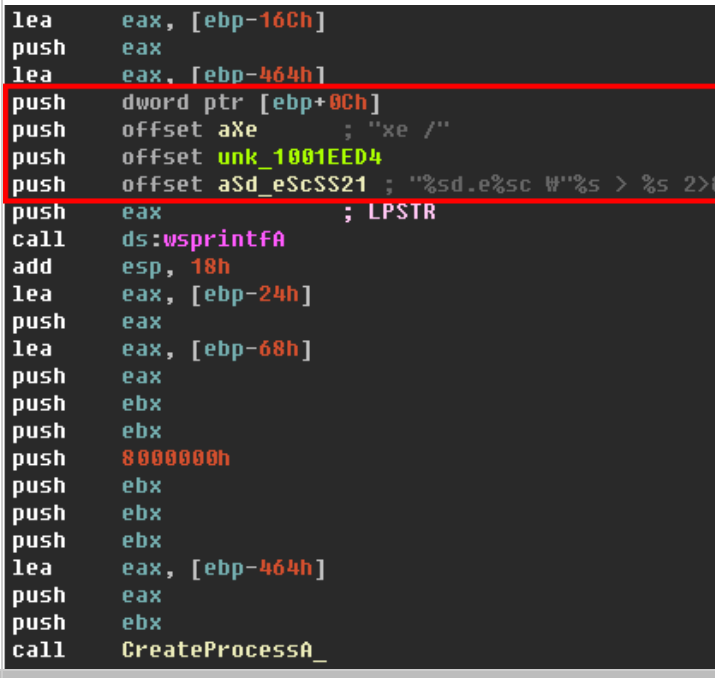
5C35360D28082E6E32D3E8EE347843F



```
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

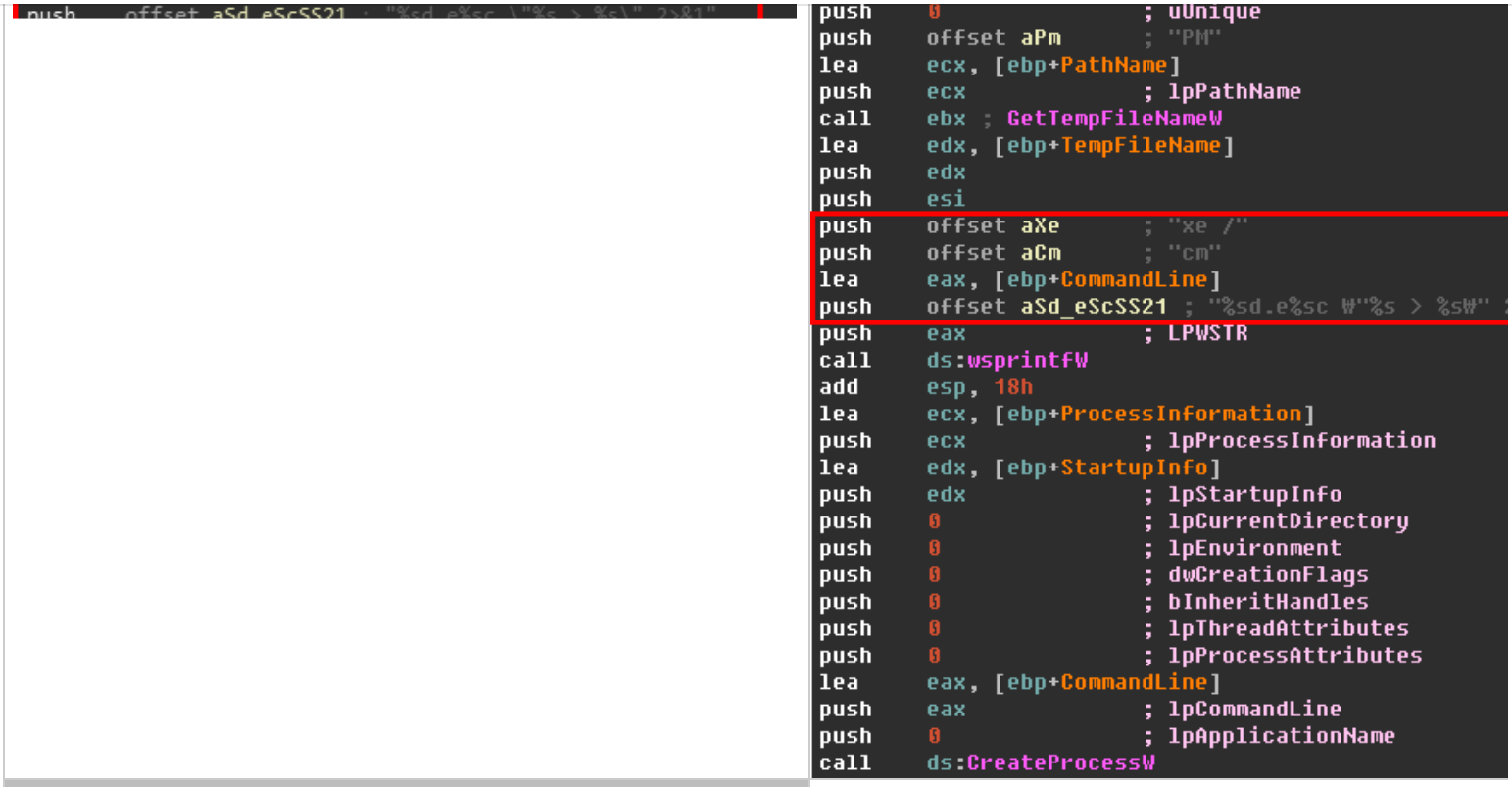


```
lea     eax, [ebp-16Ch]
push    eax
lea     eax, [ebp-464h]
push    dword ptr [ebp+0Ch]
push    offset aXe      ; "xe /"
push    offset unk_1001EED4
push    offset aSd_eScSS21 ; "%sd.e%sc W"%s > %s 2>
push    eax             ; LPSTR
call    ds:wsprintfA
add     esp, 18h
lea     eax, [ebp-24h]
push    eax
lea     eax, [ebp-68h]
push    eax
push    ebx
push    ebx
push    8000000h
push    ebx
push    ebx
push    ebx
lea     eax, [ebp-464h]
push    eax
push    ebx
call    CreateProcessA_
```

IZEX 디지털 서명을 도용한 악성코드

FA6EE9E969DF5CA4524DAA77C172A1A

ESTSECURITY



```
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 W"%s > %sW"
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                   ; lpCurrentDirectory
push    0                   ; lpEnvironment
push    0                   ; dwCreationFlags
push    0                   ; bInheritHandles
push    0                   ; lpThreadAttributes
push    0                   ; lpProcessAttributes
lea     eax, [ebp+CommandLine]
push    eax                 ; lpCommandLine
push    0                   ; lpApplicationName
call    ds:CreateProcessW
```

Ghost Puppet (gcoin2.swf)
A7C804B62AE93D708478949F498342F9

ESTSECURITY

[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**

ESTSECURITY

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 주의!

2018.09.21

사용자 정보 탈취 목적의 악성 파일이 첨부된 메일 주의

2018.09.20

스팸메일로 위장한 크립토재킹 공격 주의!

2018.09.19

Trojan.Android.Dropper 악성코드 분석 보고서

2018.09.17

댓글 0 개

이름

비밀번호

ESTsecurity

비밀글

댓글 남기기