JOINT CYBER SECURITY ADVISORY

Bundesamt für Verfassungsschutz

20 March, 2023

Warning on KIMSUKY[1] Cyber Actor's Recent Cyber Campaigns against Google's Browser and App Store Services

Summary

- The German Bundesamt für Verfassungsschutz (BfV) and the National Intelligence Service of the Republic of Korea (NIS) issue the following Joint Cyber Security Advisory to raise awareness of KIMSUKY's (a.k.a. Thallium, Velvet Chollima, etc.) cyber campaigns against Google's browser and app store services targeting experts on the Korean Peninsula and North Korea issues.

- This Cyber Security Advisory includes the strategy, modus operandi, Tactics, Techniques and Procedures (TTPs) and Indicators of Compromise (IoCs) used in KIMSUKY's campaigns that exploit Chromium-based web browser extensions and the Android app developer function.

- The BfV and NIS assess that the aforementioned actor has already targeted Korean and German entities using spear phishing emails over the last couple of years. However, considering the universally available attack method and targets of the recently observed campaign, both services believe the actor could go further by targeting global think tanks of diplomacy and security.

[1] Members of the IT security community regularly link KIMSUKY to North Korea's Reconnaissance General Bureau.

Technical Details

- As widely known, KIMSUKY has been stealing account information from the above-mentioned targets through spear phishing emails which lead to forged versions of websites disguised as the legitimate ones such as "google.com".

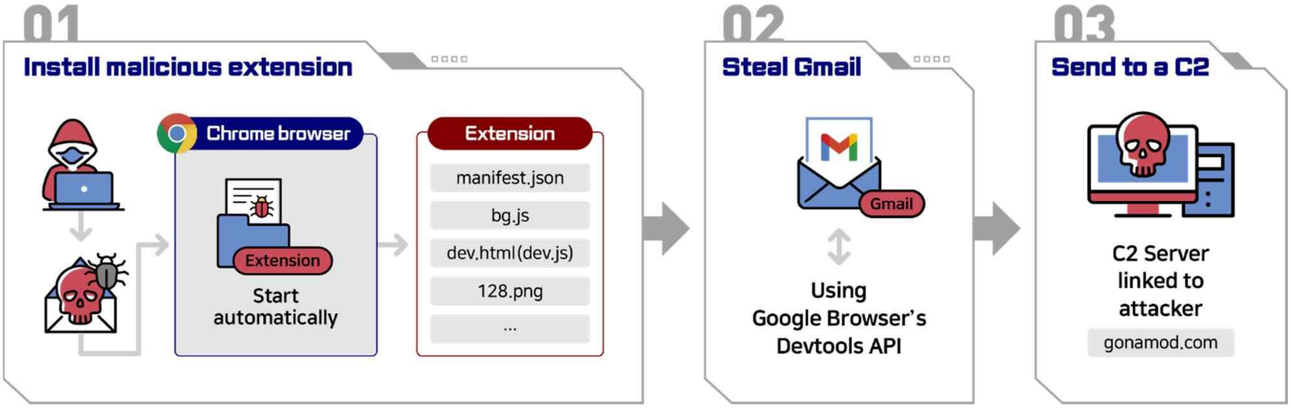
- Subsequently, the actor uses the stolen account information to impersonate acquaintances of the targets for spear phishing. Furthermore, the actor not only steals the victims' login credentials, but also personal data stored in privately used personal storage services.

- In the course of two recently observed campaigns, KIMSUKY abused web browser extension programs and legitimate Google services. The following is a brief description of the methods used by KIMSUKY.

① Stealing Google email information by using Chromium-based[2] web browsers extensions

- After installing a malicious chromium-based web browser extension program using spear phishing email, the extension program automatically operates when the victim logs in to Gmail to steal the email contents.

[2] Chromium is a free and open source web browser project, the Chromium code-base is widely used. Edge, Chrome, Whale and many other browsers are based on the Chromium code.



** Example of stealing Gmail contents in the Chrome browser*

01. Attackers entice users to install a malicious extension program by using spear phishing emails containing malicious links.

02. The installed extension program automatically steals the contents of the email account when the victim logs into their Gmail by using developer tool (Devtools API).

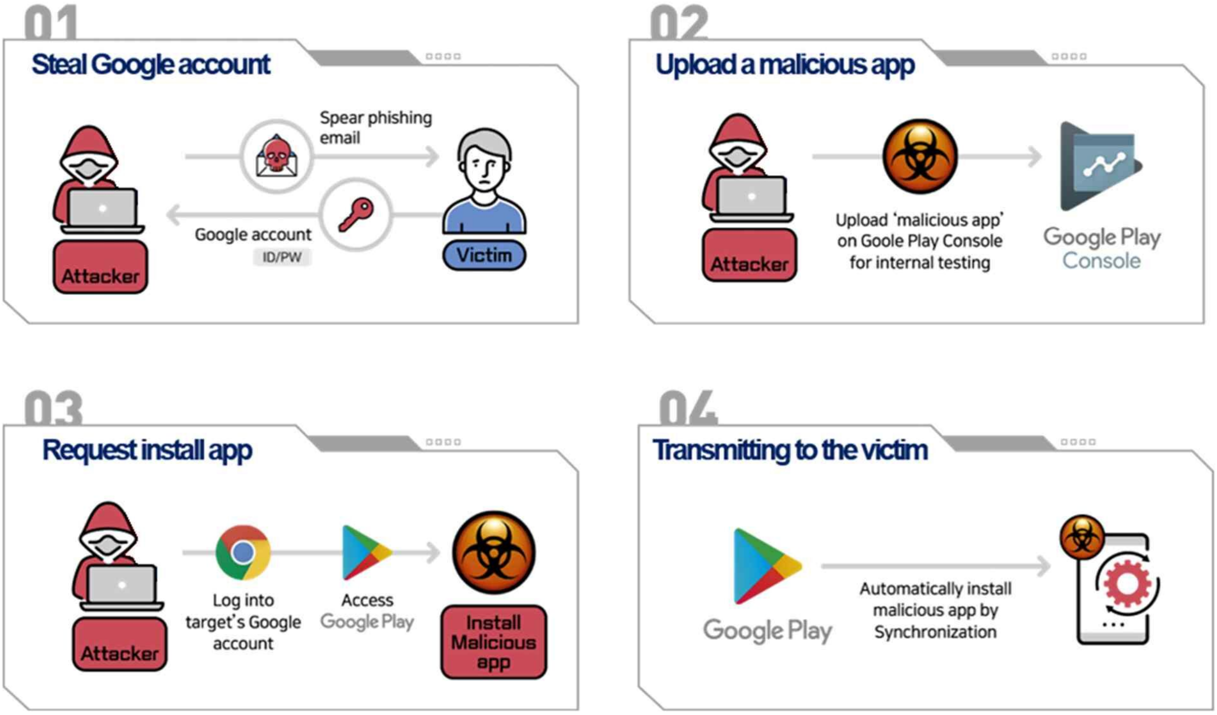
03. The content of the stolen email accounts from Gmail will be sent to the C2 server.

- Assessed goal of this technique is to secretly steal the victim's email contents, while bypassing the security settings, such as 2-factor authentication provided by the email service provider.

- When the extension is installed, an %APPDATA%AF folder is created on the victim's PC and by typing "(chrome|edge|whale)://extensions" into the URL bar, 'AF' is displayed as an extension in the list.

② Installing a malicious app on an android mobile device by exploiting Google Play's synchronization feature

- The attacker logs into the victim's Google account using the stolen login credentials. The attacker then uses the synchronization feature of Google Play. This feature allows the installation of the malicious app on the Android mobile device without any additional action by the victim.



01. The attacker steals Google account information through spear phishing email.

02. The attacker uploads a malicious app in the "Google Play Console" (comparable to an app store for applications in the development stage) for internal testing and registers victim's account as a test participant.

03. The attacker logs into the victim's account and requests the installation of the malicious app in the Google Play Store. At this point, the actor selects the target mobile device of the victim.

04. Google Play Store's synchronization feature automatically delivers the malicious app to the victim's mobile device.

- The BfV and NIS assess that the attacker's limited distributions of malicious content via the described method has been deliberate and minimizes the risk of detection.

- You can check the list of applications installed on your smartphone (refer to indicators in the Annex) to see if a malicious app is installed.

General mitigations and best practices

- Please note that included prevention guidelines in this security advisory based on the observations made by BfV and NIS on most frequent spear phishing attacks.

- Please contact the relevant authorities if a state sponsored cyber incident occurs at your organization

  South Korean organizations:

  NIS(www.nis.go.kr, 111)

  KISA(boho.or.kr, 118)

  KNPA(ecrm.police.go.kr, 182)

  German organization:

  BfV (www.verfassungsschutz.de, +49(0)228-99/792-6000)

- Enable 2-Step verification to reduce the risk of account theft.

- Since most of the attacks by KIMSUKY are being carried out through spear phishing, these attacks can more likely be avoided by taking a few precautions when receiving e-mails.

• Ways to distinguish spear phishing emails

1) First, check whether there is anything wrong with the email address

Ex)

1) @naver.com → naver-com.cc
2) @google.com → @goog1e.com
3) @daum.net → @dauum.net
4) @web.de → @webb.de
5) @gmx.net → @gnx.net

2) Do not be curious about emails sent by someone you do not know!

Ex)

1) “Request for academic cooperation”
2) “We’re interested in your opinion on ...”
3) “You won a special prize”

3) Be careful about emails you did not expect or had prior knowledge of

Ex)

1) Requests for attendance by the police
2) Information on domestic and overseas situation
3) Policy materials
4) Emails with slight context to your field of work

4) Never open an attached file you are uncertain about

Ex)

1) “New academic Research paper on...”
2) “Resume”
3) “Invoice No. 28629”
4) “Tax information”
5) “Annual income contract”

5) Should I click or not? Do not click suspicious links in your emails

Ex)

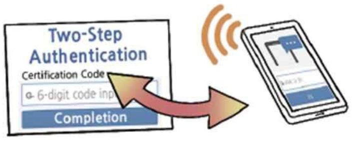
Click here ...
1) “... for detailed view of the text”
2) “... to change your password”
3) “... to check the capacity of your mail box”

- **The methods for receiving emails safely are as follows**

1) Install and update your antivirus programs

· Install and maintain the latest version of antivirus software

· Keep your computer's operating system up to date



2) Strengthen sign-in security

· Change email passwords frequently

· Sign in with multifactor authentication using One Time Passwords(OTPs)

3) Do not open suspicious emails

· Do not open emails unrelated to your work(eg. spam)

· Confirm the authenticity of the email via phone or text message

4) Do not enter your password

· Do not enter your passwords into websites linked in emails

· Visit the corresponding website directly to change the password

5) Be cautious in executing attached files

· Open the file only when it is attached to a secure email or when you were notified in advance

· For other cases, open the file after confirming the sender's authenticity

6) Check your sign-in history frequently

· Check to see whether there has been irregular sign-ins by going through your sign-in history frequently

· Actively use the "overseas login blocker" function

Indicators of Compromise

Chromium-based web browser extension program

Type	IoCs	Note
C2 servers	gonamod[.]com	HTTPS
	siekis[.]com	HTTPS
	mode=cd2&ver=3.0	HTTP param
Malicious files	012D5FFE697E33D81B9E7447F4AA338B	manifest.json
	582A033DA897C967FAADE386AC30F604	bg.js
	51527624E7921A8157F820EB0CA78E29	dev.js
	%APPDATA%\AF	Download folder
String	AF	Name of browser extension program

Abuse Google Play's synchronization feature

Type	IoCs	Note
C2 servers	navernnail[.]com	HTTP
	lowerp.onlinewebshop[.]net	HTTP
	mc.pzs[.]kr	HTTP
	23.106.122[.]16	HTTP
Malicious apps	3458DAA0DFFDC3FBB5C931F25D7A1EC0	FastViewer (com.tf.thinkdroid.secviewer)
	89F97E1D68E274B03BC40F6E06E2BA9A	Fastspy DEX File
	04BB7E1A0B4F830ED7D1377A394BC717	Fastfire (com.viewer.fastsecure)