Bundesamt für Verfassungsschutz

20. März 2023

Sicherheitshinweis zu Cyberaktivitäten und Missbrauch von Googles Browser und App Store Diensten durch KIMSUKY[1]

Zusammenfassung

- Der National Intelligence Service der Republik Korea (NIS) und das Bundesamt für Verfassungsschutz (BfV) veröffentlichen das folgende Joint Cyber Security Advisory, um auf eine Cyberspionagekampagne der Advanced Persistent Threat (APT)-Gruppe KIMSUKY aufmerksam zu machen. Die Aktivitäten zeichnen sich durch den Missbrauch von Googles Browser und App-Store Diensten gegen Forschende zum innerkoreanischen Konflikt aus.

- Dieser Sicherheitshinweis enthält Strategie, Modus Operandi, Tactics, Techniques and Procedures (TTPs) und Indikatoren (IoC) einer KIMSUKY-Spionagekampagne, die Chromium-basierte Webbrowser-Erweiterungen (Extensions) und die Android-App-Entwicklerfunktion ausnutzt.

- Nach Einschätzung von NIS und BfV hat der Akteur in den letzten Jahren bereits gezielt koreanische und deutsche Einrichtungen mit Spear-Phishing-E-Mails angegriffen. In Anbetracht der Ziele und der universell einsetzbaren Angriffsmethode gehen beide Dienste davon aus, dass der Akteur die hier beschriebene Kampagne u.a. auf globale Think Tanks für Diplomatie und Sicherheit erweitern könnte.

[1] KIMSUKY, u.a. auch bekannt als VELVET CHOLLIMA oder THALLIUM, wird von der IT-Sicherheitscommunity regelmäßig dem nordkoreanischen Nachrichtendienst RGB zugeschrieben.

Technische Beschreibung

- Das bevorzugte Vorgehen der Cybergruppierung ist gut dokumentiert. KIMSUKY stiehlt von den oben genannten Zielen und Personen Kontoinformationen durch Spear-Phishing-E-Mails, die zu gefälschten, als legitim getarnten Versionen von Websites, wie z. B. "google.com", führen.

- Anschließend nutzt der Akteur die gestohlenen Kontoinformationen, um weitere Spear-Phishing-Angriffe durchzuführen. Dabei stiehlt der Akteur nicht nur die Anmeldedaten der Opfer, sondern auch darüber hinaus gehende persönliche Daten, die bei privat genutzten Datenspeicherdiensten gesichert sind.

- Im Rahmen von zwei kürzlich beobachteten Cyberspionagekampagnen missbrauchte KIMSUKY Webbrowser Extensions und legitime Funktionen von Google-Diensten.

① Erbeutung von Google E-Mail-Informationen durch Chromium[2] Webbrowser Extensions

- Mithilfe einer Spear-Phishing-E-Mail wird die Zielperson zur Installation einer maliziösen, auf Chromium basierenden Webbrowser Extension verleitet. In der Folge wird das Programm automatisch aktiviert, wenn sich das Opfer bei Google Mail (Gmail) anmeldet, und stiehlt Login-Credentials sowie den Inhalt des E-Mail-Postfachs.

[2] Chromium ist ein kostenloses Open-Source Webbrowser Projekt. Chromium Code ist die Basis von vielen weiteren Browsern, darunter Edge, Chrome und Whale.

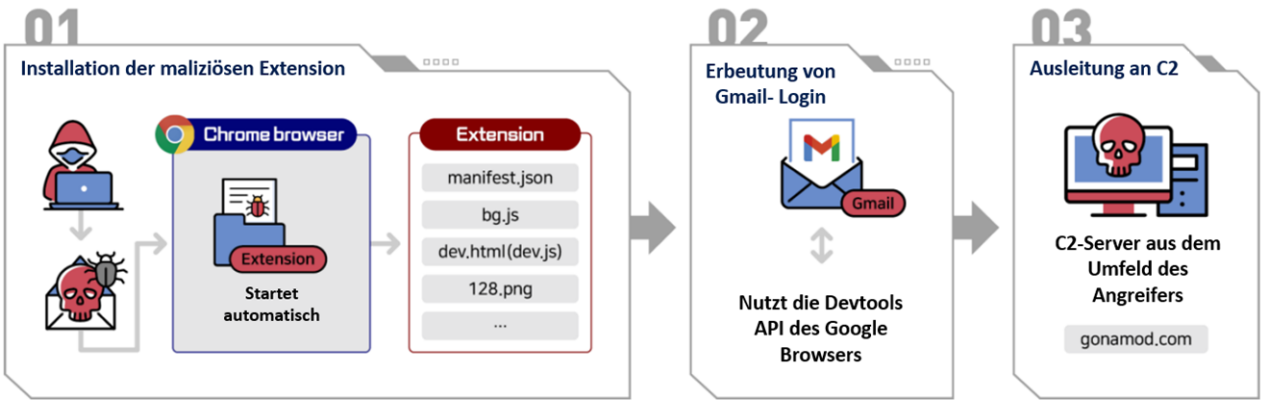


Abbildung 1: Beispiel von Credential Stealing.

01. Akteur verleitet die Zielperson durch Spear-Phishing-E-Mails mit schadhaften Links zur Installation einer maliziösen Webbrowser Extension.

02. Die installierte Extension greift durch Entwicklertools (Devtools API) automatisch den Inhalt des Gmail-Postfaches ab, wenn das Opfer sich einloggt.

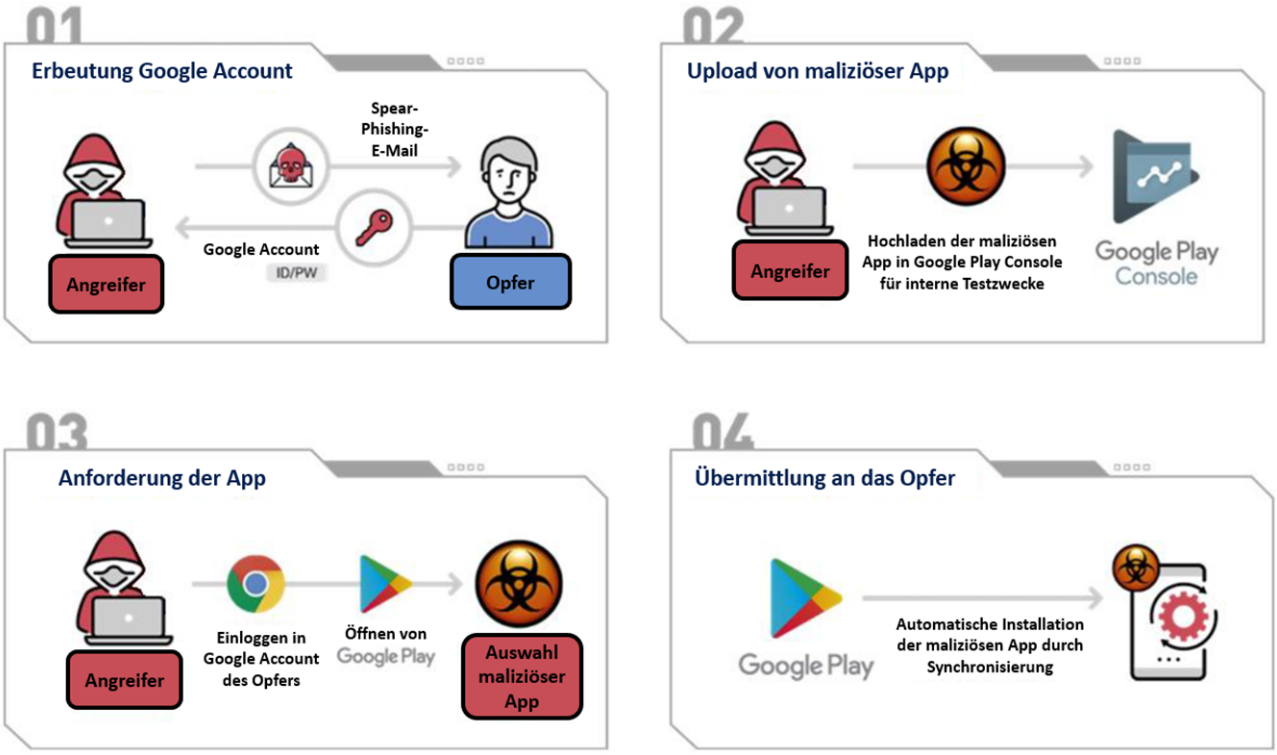
03. Der Inhalt des kompromittierten Gmail-Accounts wird an einen C2-Server ausgeleitet.

- Ziel des Vorgehens ist das unbemerkte Erbeuten der Inhalte des E-Mail-Postfachs des Opfers. Dabei werden gängige Sicherheitsvorkehrungen der E-Mail-Provider, wie beispielsweise Zwei-Faktor-Authentifizierung, umgangen.

- Bei Installation der maliziösen Extension wird auf dem PC des Opfers der Ordner %APPDATA%AF erstellt. Die Installation kann durch die Eingabe “(chrome|edge|whale)://extensions” in der URL-Leiste des Browsers überprüft werden.

② Installation einer maliziösen App auf einem Android-Mobilgerät durch Missbrauch der Synchronisierungsfunktion von Google Play

- Der Akteur loggt sich mit den erbeuteten Credentials in den Google Account des Opfers ein. In den Einstellungen des Accounts aktiviert er die Synchronisierungsfunktion von Google Play. Dieses Feature erlaubt die Installation der maliziösen App ohne zusätzliches Zutun des Opfers.



01. Akteur erbeutet durch Spear-Phishing-Angriff die Accountdaten des Opfers.

02. Akteur lädt in der “Google Play Console” für interne Testzwecke (vergleichbar mit App Store für Apps in der Entwicklungsphase) die maliziöse App hoch. Der Google Account des Opfers wird als Testteilnehmer hinzugefügt.

03. Akteur loggt sich in den Account des Opfers ein und fordert die Installation der maliziösen App über den Google Play Store an und wählt das Installationsziel (Android Mobilgerät des Opfers) aus.

04. Die Synchronisierungsfunktion des Google Play Store installiert die maliziöse App automatisch auf dem Mobilgerät des Opfers.

- Zum derzeitigen Zeitpunkt wird davon ausgegangen, dass der Akteur mit der hier beschriebenen Methode bislang nur in begrenztem Umfang Angriffe durchführt, um das Risiko einer Entdeckung zu minimieren.

- Sie können über die Einstellungen Ihres Mobilgerätes eine Liste der vorhandenen Apps aufrufen, um zu prüfen, ob eines der maliziösen Programme (siehe Indikatorenliste) installiert ist.

Allgemeine Sicherheitsmaßnahmen und Best Practices

- Bitte beachten Sie die folgenden Präventionshinweise von NIS und BfV zu häufig beobachteten Spear-Phishing-Angriffen.

- Bitte wenden Sie sich an die jeweiligen zuständigen Behörden, wenn Ihre Organisation Ziel eines möglicherweise staatlich gesteuerten Cyberangriffs wird

  Deutschland

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

  Südkorea:

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

  KISA(boho.or.kr, 118)

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

- Nutzen Sie wenn möglich Zwei-Faktor-Authentifizierung, um Ihre Accounts zu schützen.

- Da die meisten Angriffe von KIMSUKY über Spear-Phishing durchgeführt werden, können einige Vorsichtsmaßnahmen beim Empfang von E-Mails das Risiko eines erfolgreichen Angriffs minimieren.

• Erkennen einer Spear-Phishing-E-Mail

1) Prüfen Sie die Absenderadresse sorgfältig.

Bsp.)

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) Hinterfragen Sie verlockende E-Mail-Betreffs!

Bsp.)

1) “Anfrage zu akademischer Zusammenarbeit”
2) “Wir interessieren uns für Ihre Einschätzung zu …”
3) “Sie haben gewonnen”

3) Seien Sie vorsichtig bei E-Mails, deren Eingang Sie nicht erwarten.

Bsp.)

1) Vorladungen von Polizei oder Behörden
2) Informationen zu nationaler oder internationaler Lage
3) Strategische politische Informationen

4) Öffnen Sie keine Anhänge, wenn Sie sich unsicher sind.

Bsp.)

1) “Neue Forschungsarbeit zu…”
2) “Résumé”
3) “Rechnung Nr. 28629”
4) “Steuerbescheid”
5) “Arbeitsangebot mit Vergütung”

5) Klicken Sie keine unbekannten Links an.

Bsp.)

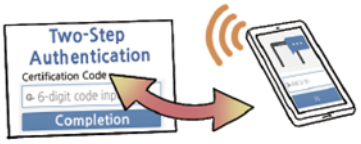
“Klicken Sie hier …

1) … um den ganzen Text zu lesen”
2) … um Ihr Passwort zu ändern”
3) … um die Kapazität Ihres Postfachs zu sehen”

- **Allgemeine Sicherheitshinweise beim Empfangen von E-Mails**

1) Installieren und Updaten eines Antivirenprogramms

- Achten Sie darauf, Ihr Antivirenprogramm zu updaten.
- Regelmäßiges Updaten Ihres Betriebssystems.



2) Verbesserung der Login-Sicherheit

- Ändern Sie regelmäßig Ihr Passwort.
- Anmeldung mit Multifaktor-Authentifizierung über Einmal-Passwörter (OTPs)

3) Öffnen Sie keine verdächtigen Emails

- Öffnen Sie keine E-Mails, die Ihnen unbekannt sind (z.B. Spam).
- Überprüfen Sie Absender durch einen Anruf oder eine Textnachricht.

4) Geben Sie Ihr Passwort nicht preis

- Geben Sie Ihr Passwort nicht auf in E-Mails verlinkten Websites ein.
- Besuchen Sie zum Ändern Ihres Passworts die jeweilige Website direkt.

5) Seien Sie vorsichtig beim Öffnen oder Ausführen von Anhängen

- Öffnen Sie nur Anhänge von sicheren E-Mails oder wenn Ihnen die Datei angekündigt wurde.
- Öffnen Sie Dateien erst, nachdem Sie die Absenderidentität geprüft haben.

6) Überprüfen Sie Ihren Anmeldeverlauf

- Prüfen Sie Ihren Anmeldeverlauf regelmäßig auf verdächtige Aktivität.
- Nutzen Sie wenn möglich die Funktion "Übersee-Login-Blocker".

Indicators of Compromise

Chromium-basierte Webbrowser Extension

Art	IoCs	Bemerkung
C2 Server	gonamod[.]com	HTTPS
	siekis[.]com	HTTPS
	mode=cd2&ver=3.0	HTTP param
Maliziöse Dateien	012D5FFE697E33D81B9E7447F4AA338B	manifest.json
	582A033DA897C967FAADE386AC30F604	bg.js
	51527624E7921A8157F820EB0CA78E29	dev.js
	%APPDATA%\AF	Download Ordner
String	AF	Name der Webbrowser Extension

Missbrauch von Google Plays Synchronisierungsfunktion

Art	IoCs	Bemerkung
C2 Server	navernnail[.]com	HTTP
	lowerp.onlinewebshop[.]net	HTTP
	mc.pzs[.]kr	HTTP
	23.106.122[.]16	HTTP
Maliziöse Apps	3458DAA0DFFDC3FBB5C931F25D7A1EC0	FastViewer (com.tf.thinkdroid.secviewer)
	89F97E1D68E274B03BC40F6E06E2BA9A	Fastspy DEX File
	04BB7E1A0B4F830ED7D1377A394BC717	Fastfire (com.viewer.fastsecure)