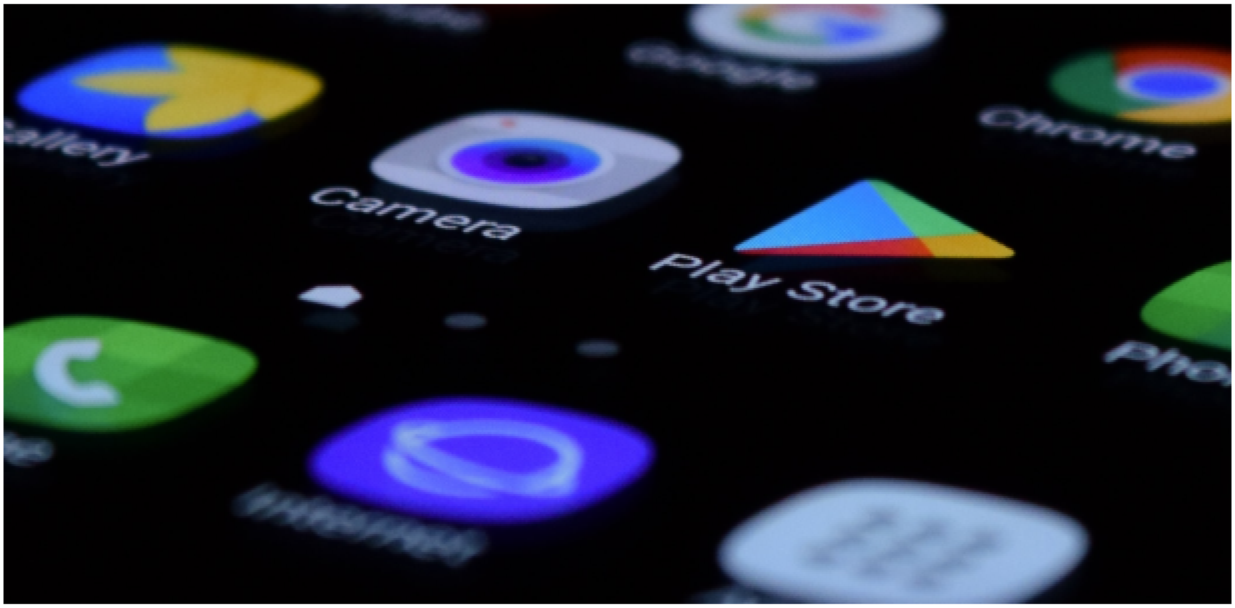
New HiddenAds malware affects 1M+ users and hides on the Google Play Store

mcafee.com/blogs/other-blogs/mcafee-labs/new-hiddenads-malware-that-runs-automatically-and-hides-on-google-play-1m-users-affected/

July 29, 2022



McAfee Labs

Jul 28, 2022

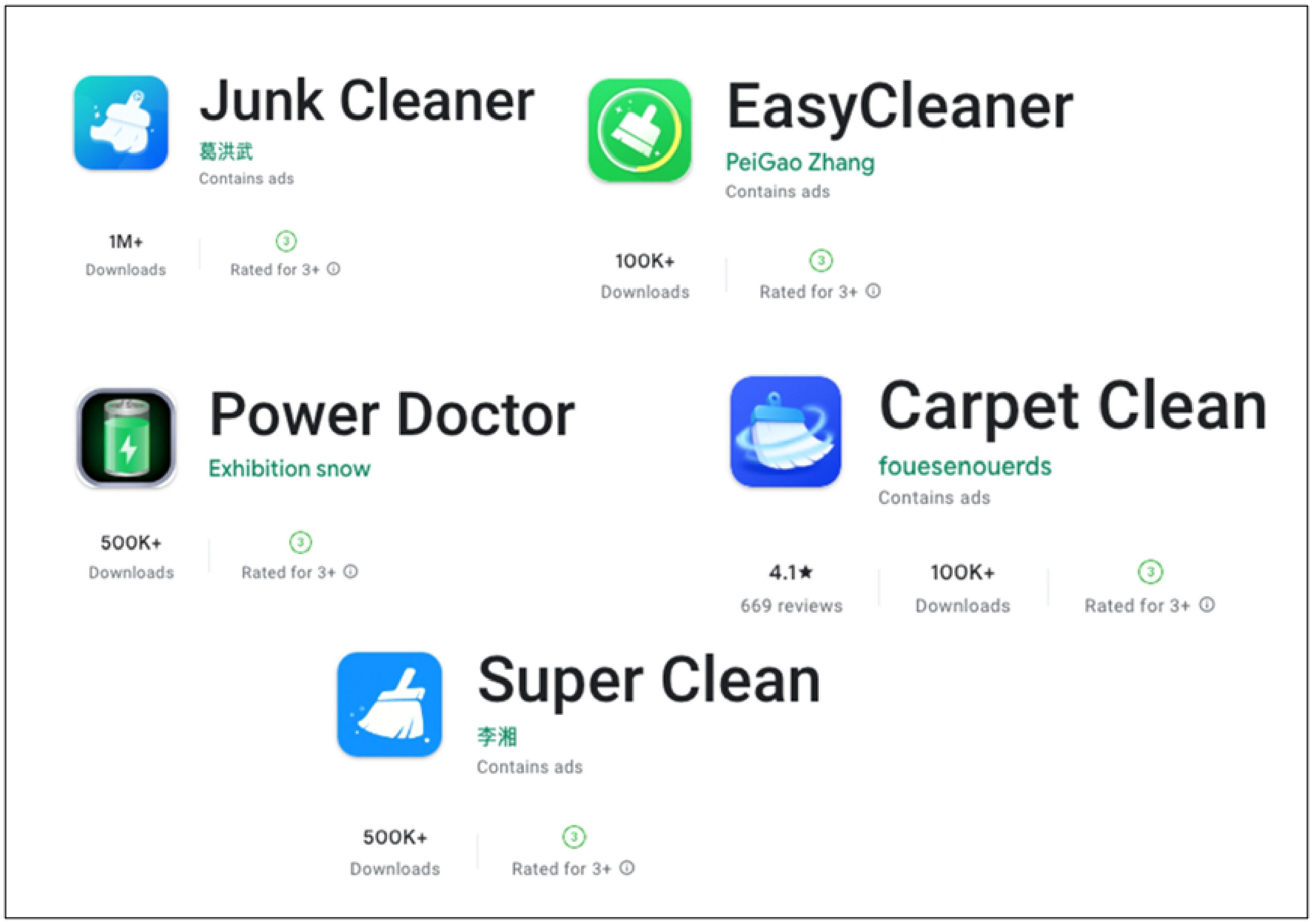
6 MIN READ

Authored by Dexter Shin

McAfee's Mobile Research Team has identified new malware on the Google Play Store. Most of them are disguising themselves as cleaner apps that delete junk files or help optimize their batteries for device management. However, this malware hides and continuously show advertisements to victims. In addition, they run malicious services automatically upon installation without executing the app.

HiddenAds functions and promotion

They exist on Google Play even though they have malicious activities, so the victim can search for the following apps to optimize their device.



Junk Cleaner
葛洪武
Contains ads
1M+ Downloads
Rated for 3+

EasyCleaner
PeiGao Zhang
Contains ads
100K+ Downloads
Rated for 3+

Power Doctor
Exhibition snow
500K+ Downloads
Rated for 3+

Carpet Clean
fouesenouerds
Contains ads
4.1★ 669 reviews
100K+ Downloads
Rated for 3+

Super Clean
李湘
Contains ads
500K+ Downloads
Rated for 3+

Figure 1. Malware on Google Play

Users may generally think installing the app without executing it is safe. But you may have to change your mind because of this malware. When you install this malware on your device, it is executed without interaction and executes a malicious service.

In addition, they try to hide themselves to prevent users from noticing and deleting apps. Change their icon to a Google Play icon that users are familiar with and change its name to 'Google Play' or 'Setting.'

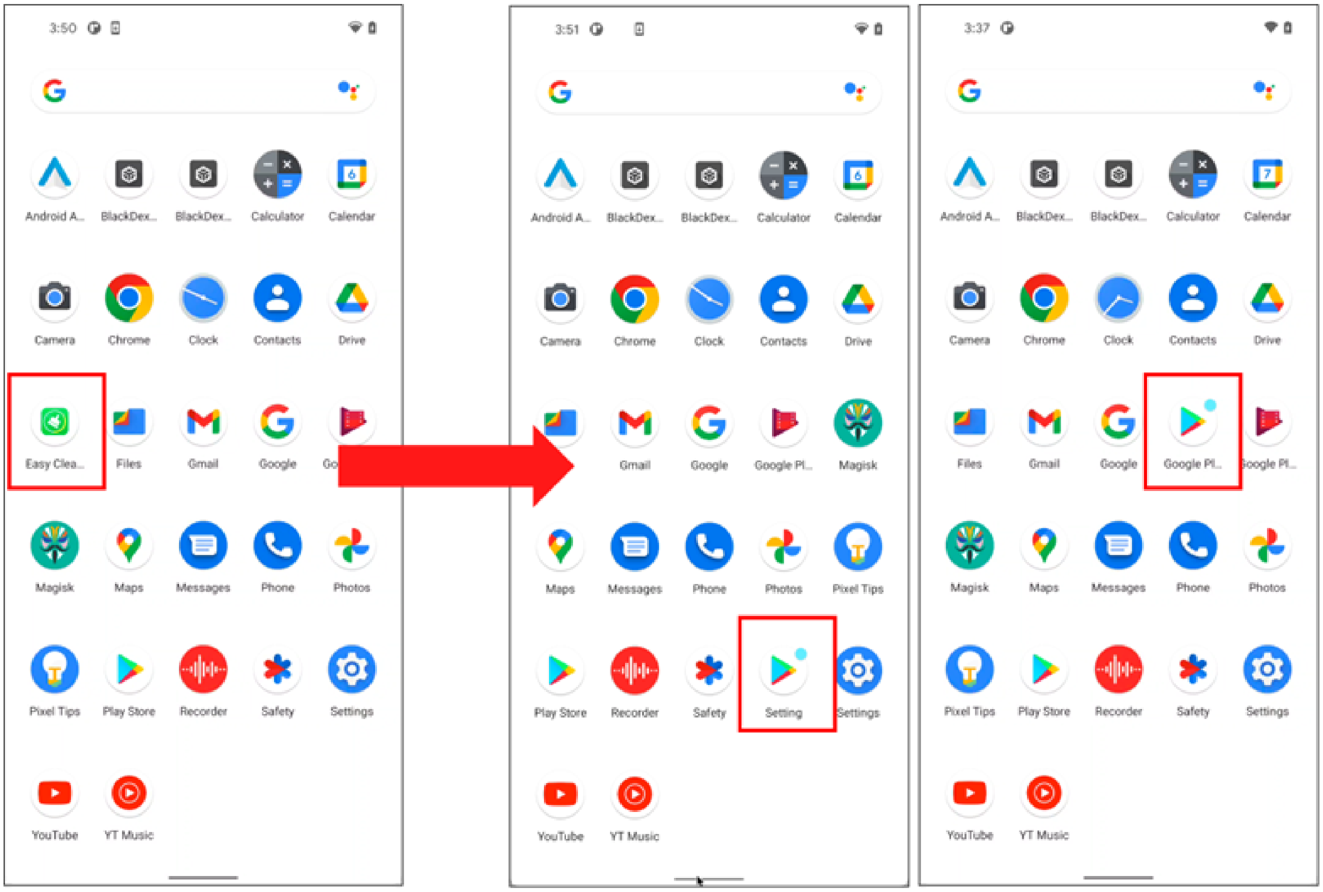


Figure 2. The Malware hides itself by changing icons and names

Automatically executed services constantly display advertisements to victims in a variety of ways.

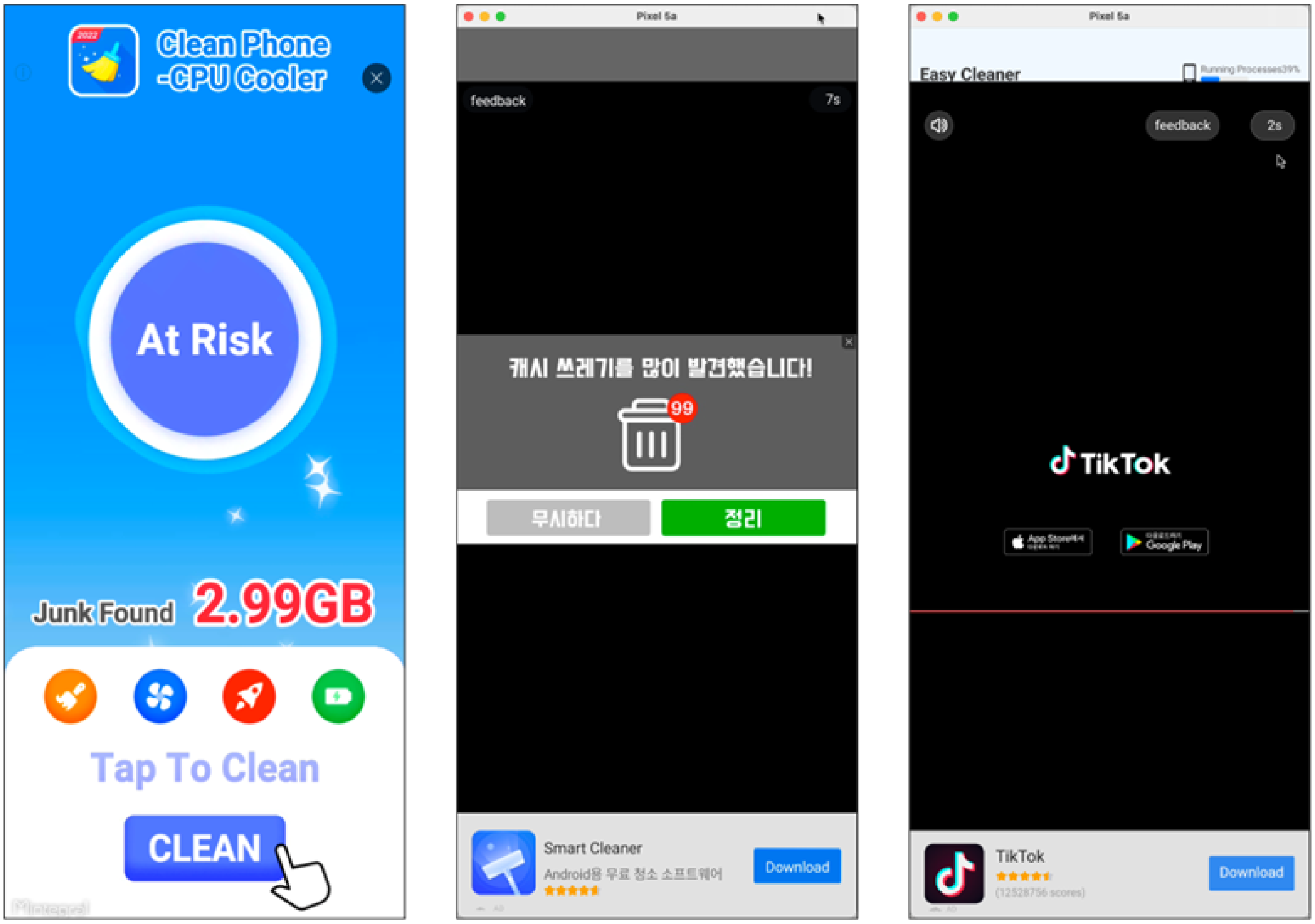
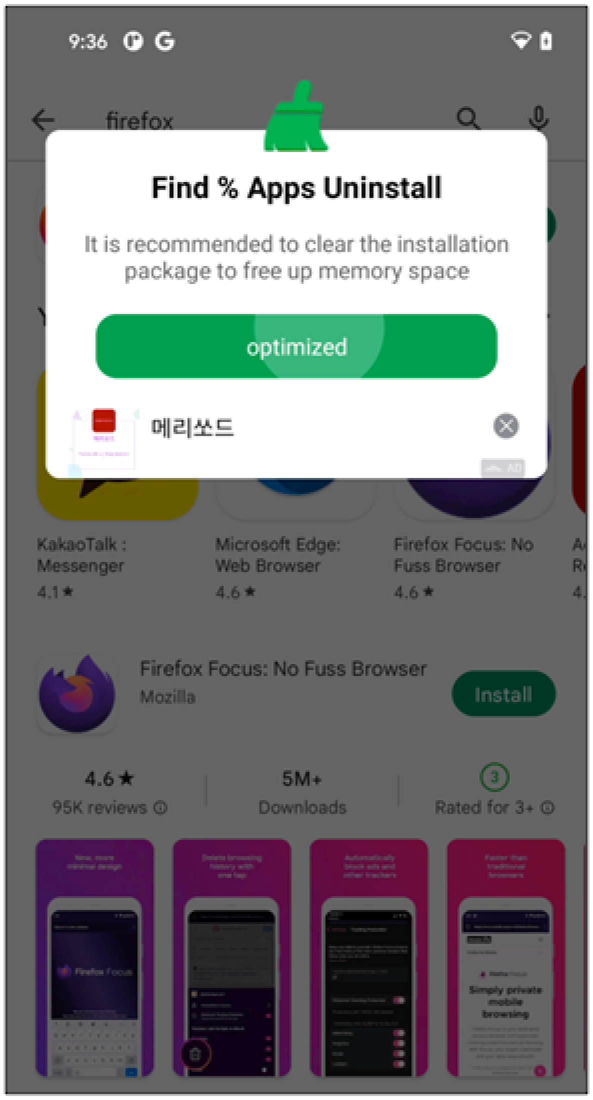
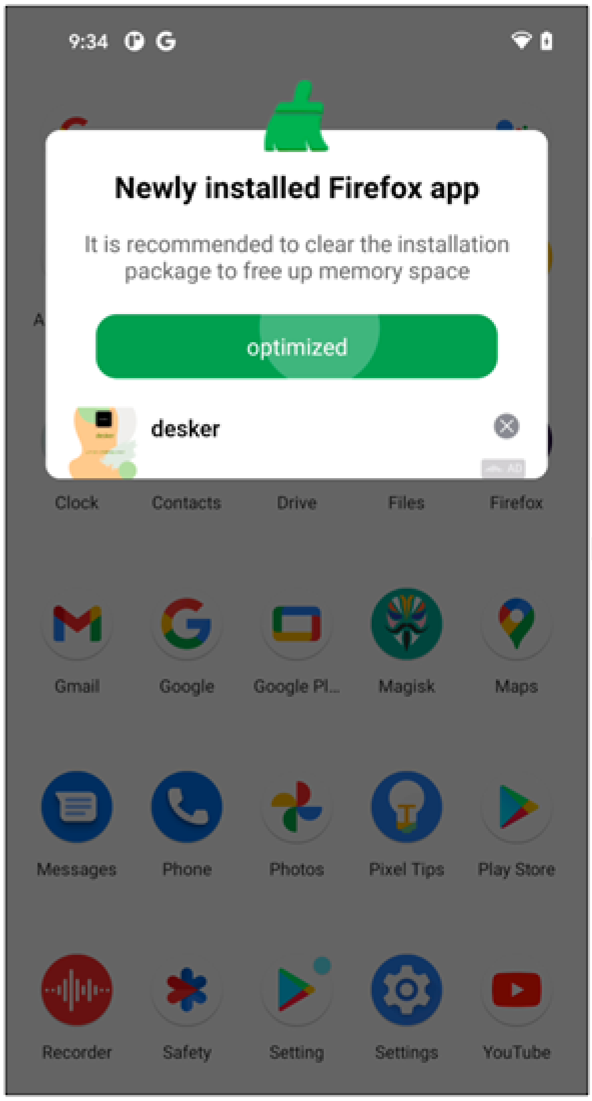


Figure 3. A sudden display of advertisements

These services also induce users to run an app when they install, uninstall, or update apps on their devices.



9:36
firefox
Find % Apps Uninstall
It is recommended to clear the installation package to free up memory space
optimized
메리쏘드
AD
KakaoTalk : Messenger
4.1★
Microsoft Edge: Web Browser
4.6★
Firefox Focus: No Fuss Browser
4.6★
Firefox Focus: No Fuss Browser
Mozilla
Install
4.6★
95K reviews
5M+
Downloads
3
Rated for 3+
Simply private mobile browsing

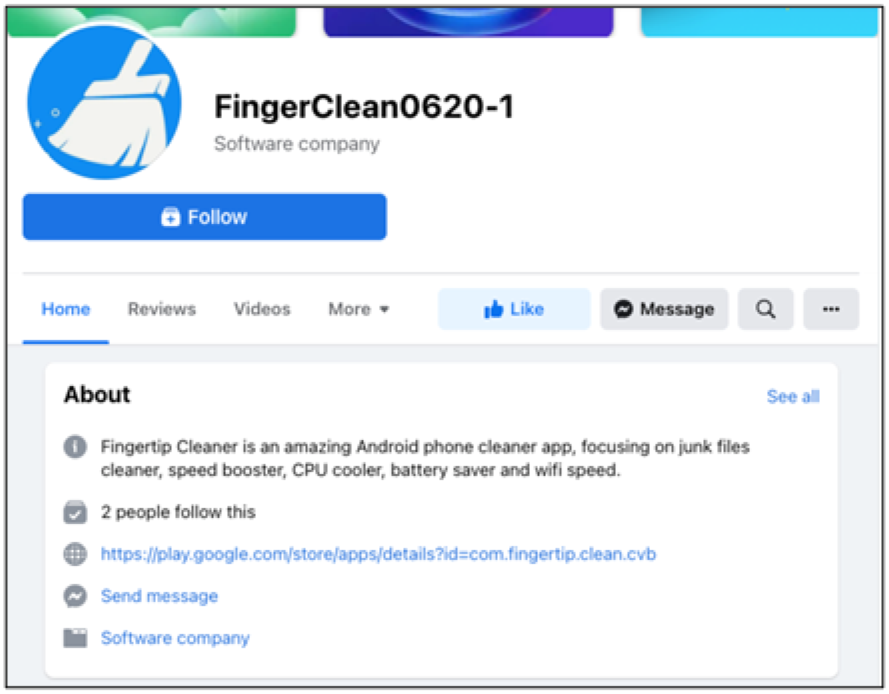


Newly installed Firefox app

It is recommended to clear the installation package to free up memory space

Figure 4. A button to induce users to run app

To promote these apps to new users, the malware authors created advertising pages on Facebook. Because it is the link to Google Play distributed through legitimate social media, users will download it without a doubt.



FingerClean0620-1

Software company

About

See all

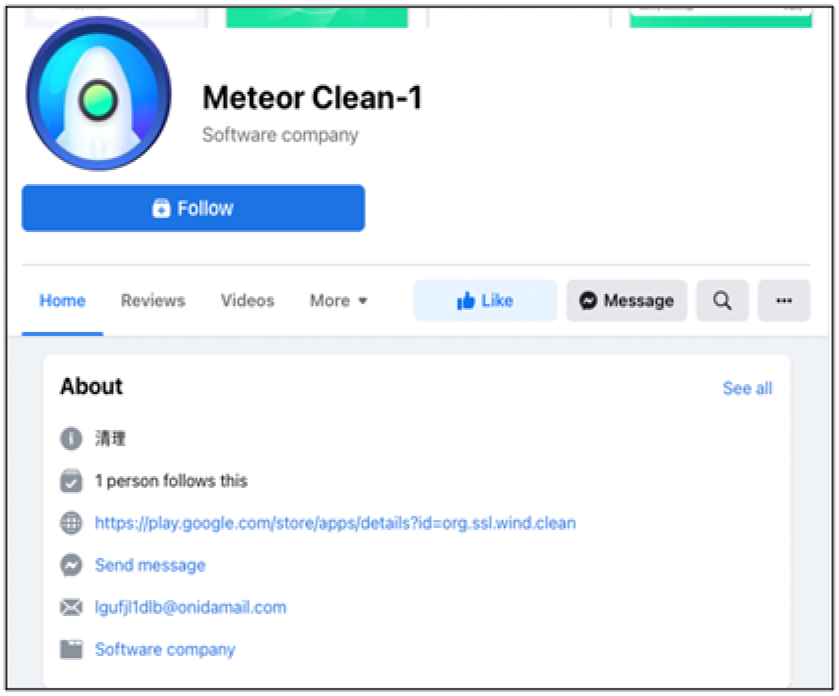
Fingertip Cleaner is an amazing Android phone cleaner app, focusing on junk files cleaner, speed booster, CPU cooler, battery saver and wifi speed.

2 people follow this

https://play.google.com/store/apps/details?id=com.fingertip.clean.cvb

Send message

Software company



Meteor Clean-1

Software company

About

See all

清理

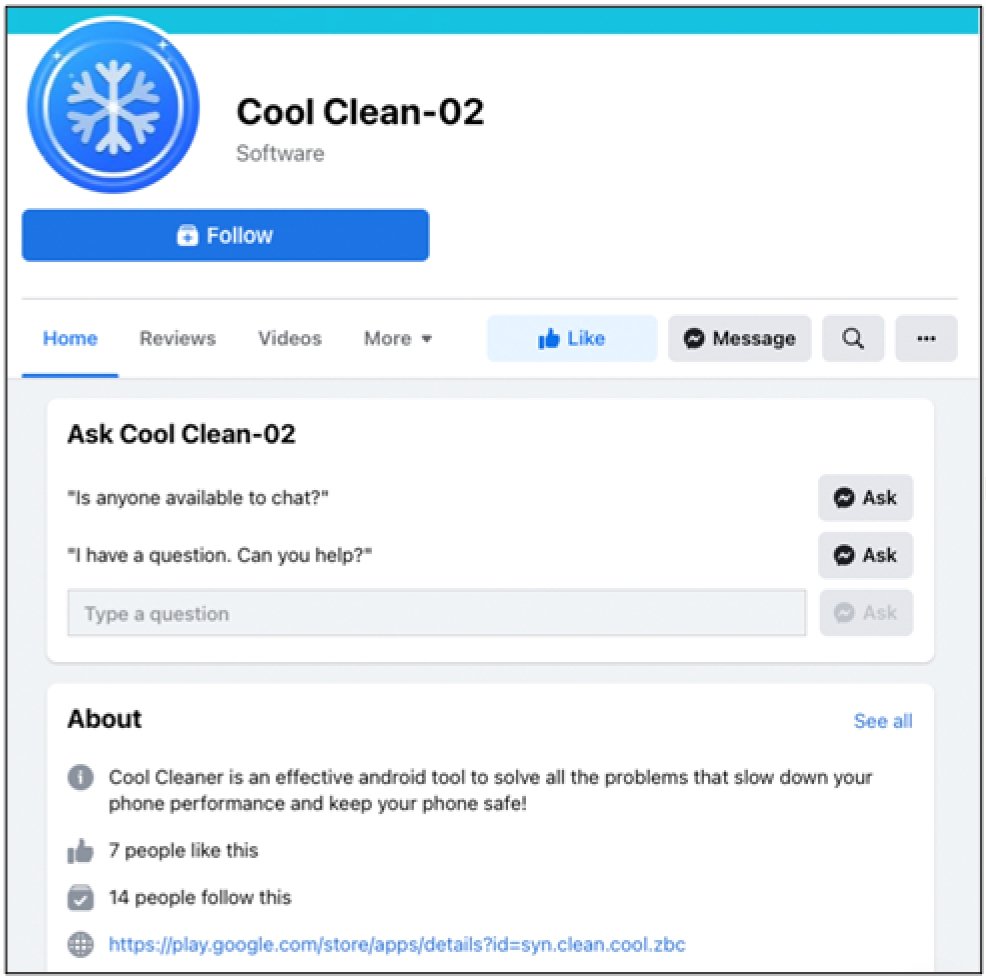
1 person follows this

https://play.google.com/store/apps/details?id=org.ssl.wind.clean

Send message

lgufjl1dlb@onidamail.com

Software company



Cool Clean-02

Software

Ask Cool Clean-02

"Is anyone available to chat?"

"I have a question. Can you help?"

Type a question

About

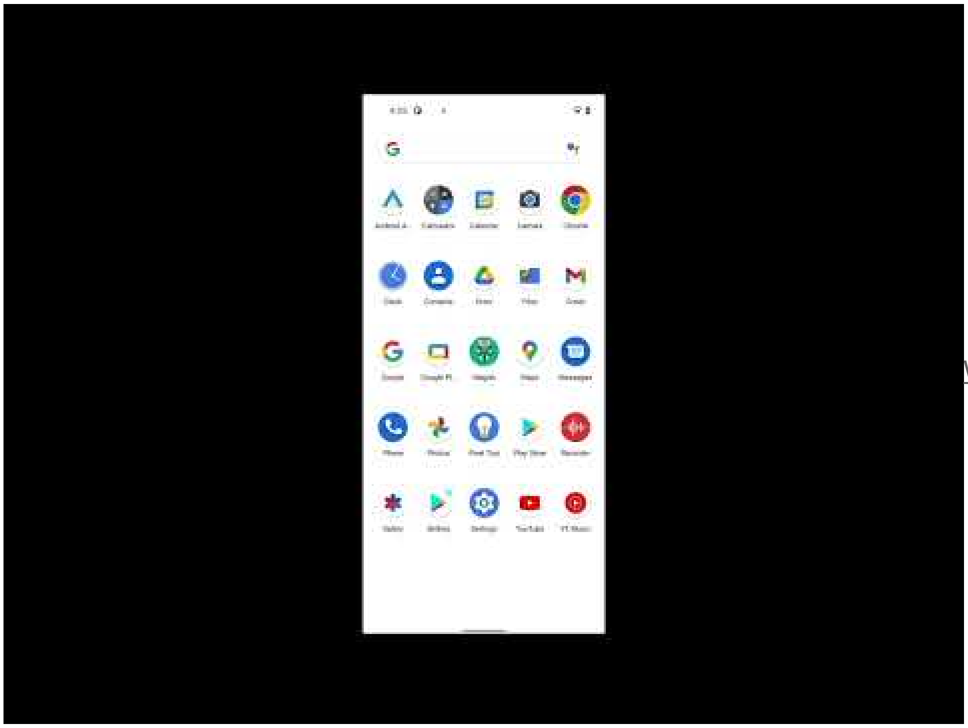
Cool Cleaner is an effective android tool to solve all the problems that slow down your phone performance and keep your phone safe!

7 people like this

14 people follow this

https://play.google.com/store/apps/details?id=syn.clean.cool.zbc

Figure 5. Advertising pages on Facebook

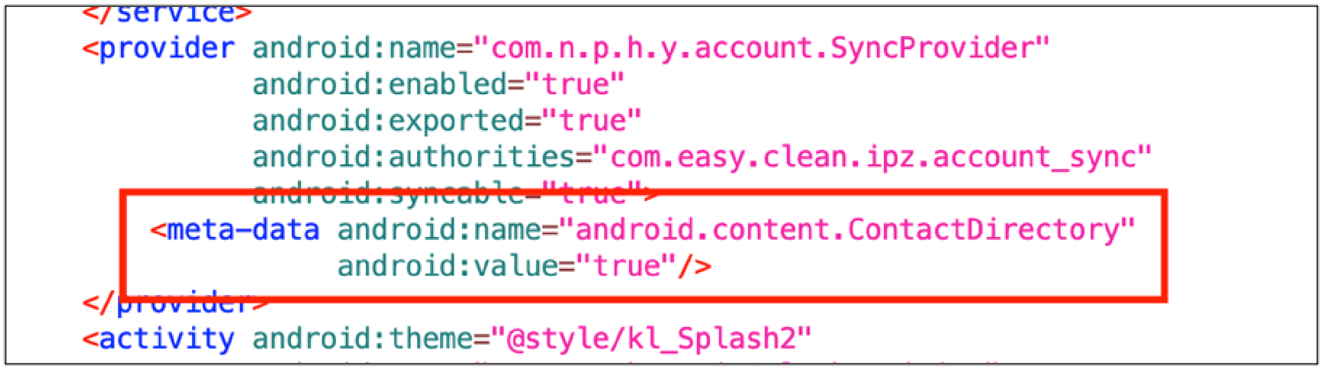


Watch Video At:

https://youtu.be/A0J7Fb1Y-CI

How it works

This malware uses the Contact Provider. The Contact Provider is the source of data you see in the device's contacts application, and you can also access its data in your own application and transfer data between the device and online services. For this, Google provides ContactsContract class. ContactsContract is the contract between the Contacts Provider and applications. In ContactsContract, there is a class called Directory. A Directory represents a contacts corpus and is implemented as a Content Provider with its unique authority. So, developers can use it if they want to implement a custom directory. The Contact Provider can recognize that the app is using a custom directory by checking special metadata in the manifest file.

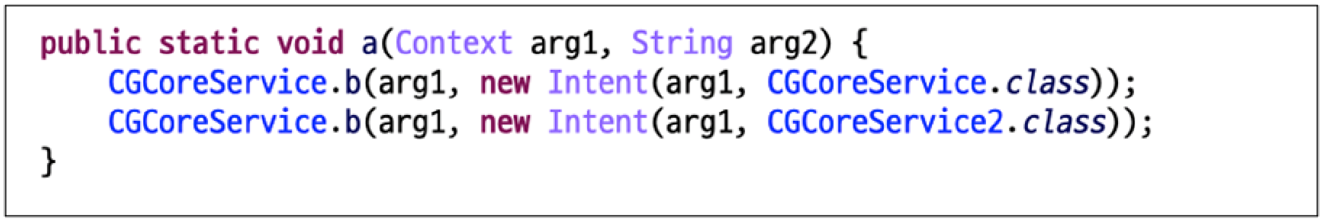


```
    </service>
    <provider android:name="com.n.p.h.y.account.SyncProvider"
              android:enabled="true"
              android:exported="true"
              android:authorities="com.easy.clean.ipz.account_sync"
              android:syncable="true">
        <meta-data android:name="android.content.ContactDirectory"
                   android:value="true"/>
    </provider>
    <activity android:theme="@style/kl_Splash2"
```

Figure 6. Content providers declared with special metadata in manifest

The important thing is the Contact Provider automatically interrogates newly installed or replaced packages. Thus, installing a package containing special metadata will always call the Contact Provider automatically.

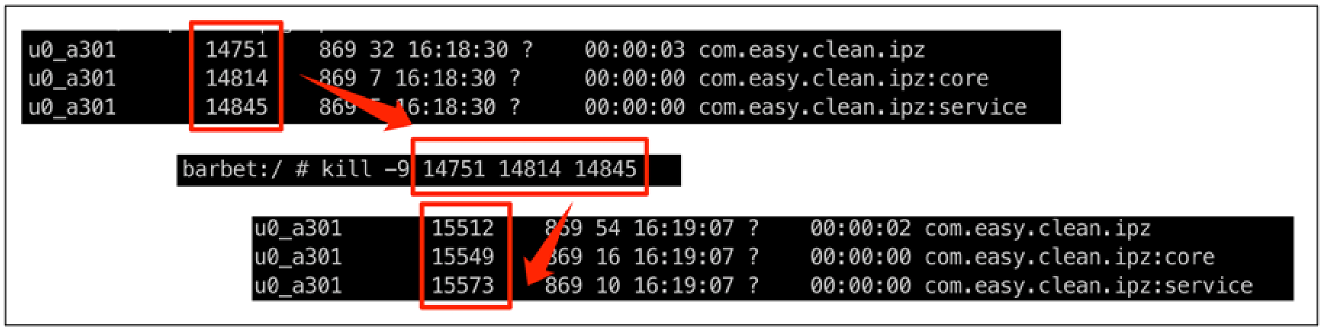
The first activity defined in the application tag in the manifest file is executed as soon as you install it just by declaring the metadata. The first activity of this malware will create a permanent malicious service for displaying advertisements.



```
public static void a(Context arg1, String arg2) {
    CGCoreService.b(arg1, new Intent(arg1, CGCoreService.class));
    CGCoreService.b(arg1, new Intent(arg1, CGCoreService2.class));
}
```

Figure 7. Create a malicious service for displaying ads

In addition, the service process will generate immediately even if it is forced to kill.



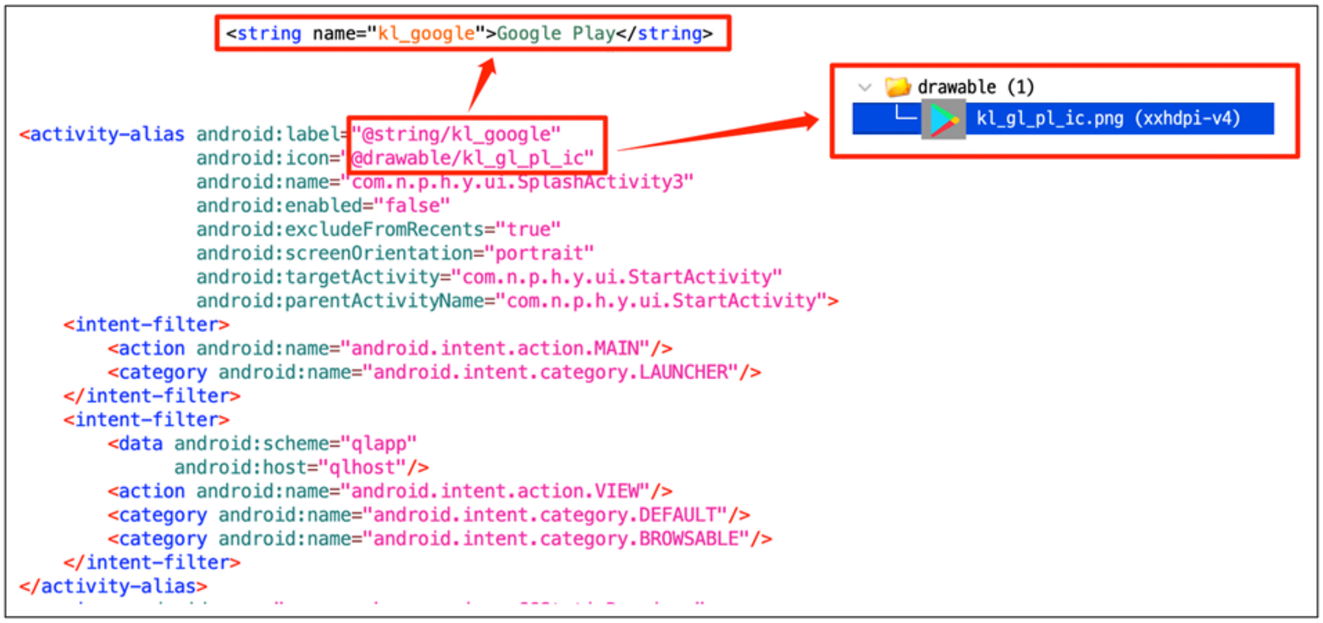
```
u0_a301        14751   869 32 16:18:30 ?    00:00:03 com.easy.clean.ipz
u0_a301        14814   869 7 16:18:30 ?     00:00:00 com.easy.clean.ipz:core
u0_a301        14845   869 5 16:18:30 ?     00:00:00 com.easy.clean.ipz:service

barbet:/ # kill -9 14751 14814 14845

u0_a301        15512   869 54 16:19:07 ?    00:00:02 com.easy.clean.ipz
u0_a301        15549   869 16 16:19:07 ?    00:00:00 com.easy.clean.ipz:core
u0_a301        15573   869 10 16:19:07 ?    00:00:00 com.easy.clean.ipz:service
```

Figure 8. Malicious service process that continues to generate

Next, they change their icons and names using the <activity-alias> tag to hide.



```
<string name="kl_google">Google Play</string>

<activity-alias android:label="@string/kl_google"
                android:icon="@drawable/kl_gl_pl_ic"
                android:name="com.n.p.h.y.ui.SplashActivity3"
                android:enabled="false"
                android:excludeFromRecents="true"
                android:screenOrientation="portrait"
                android:targetActivity="com.n.p.h.y.ui.StartActivity"
                android:parentActivityName="com.n.p.h.y.ui.StartActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
    <intent-filter>
        <data android:scheme="qlapp"
              android:host="qlhost"/>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE"/>
    </intent-filter>
</activity-alias>
```

Figure 9. Using tags to change app icons and names

Users infected worldwide

It is confirmed that users have already installed these apps from 100K to 1M+. Considering that the malware works when it is installed, the installed number is reflected as the victim's number. According to McAfee telemetry data, this malware and its variants affect a wide range of countries, including South Korea, Japan, and Brazil:

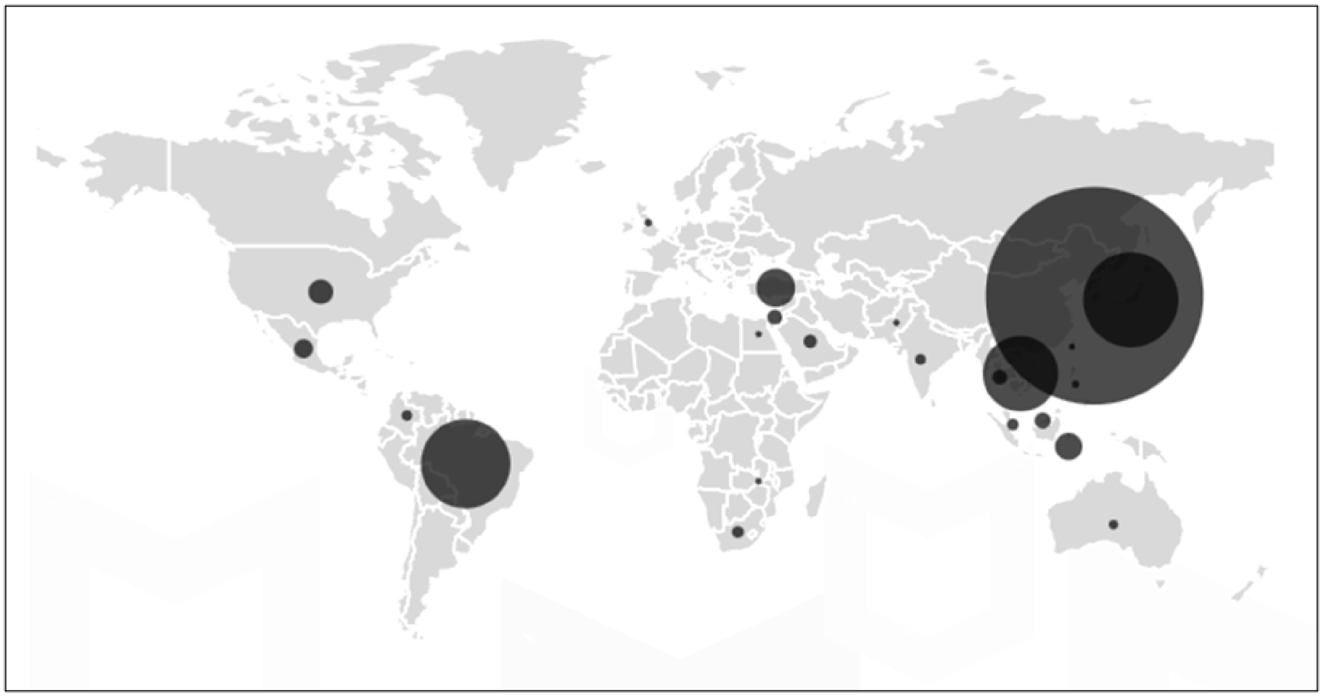


Figure 10. Top affected countries include South Korea, Japan, and Brazil

Conclusion

This malware is auto-starting malware, so as soon as the users download it from Google Play, they are infected immediately. And it is still constantly developing variants that are published by different developer accounts. Therefore, it is not easy for users to notice this type of malware.

We already disclosed this threat to Google and all reported applications were removed from the Play Store. Also, McAfee Mobile Security detects this threat as Android/HiddenAds and protects you from this type of malware. For more information about McAfee Mobile Security, visit https://www.mcafeemobilesecurity.com

Indicators of Compromise

Applications:

App Name	Package Name	Downloads
Junk Cleaner	cn.junk.clean.plp	1M+
EasyCleaner	com.easy.clean.ipz	100K+
Power Doctor	com.power.doctor.mnb	500K+
Super Clean	com.super.clean.zaz	500K+
Full Clean -Clean Cache	org.stemp.fll.clean	1M+

Fingertip Cleaner	com.fingertip.clean.cvb	500K+
Quick Cleaner	org.qck.cle.oyo	1M+
Keep Clean	org.clean.sys.lunch	1M+
Windy Clean	in.phone.clean.www	500K+
Carpet Clean	og.crp.cln.zda	100K+
Cool Clean	syn.clean.cool.zbc	500K+
Strong Clean	in.memory.sys.clean	500K+
Meteor Clean	org.ssl.wind.clean	100K+

SHA256:

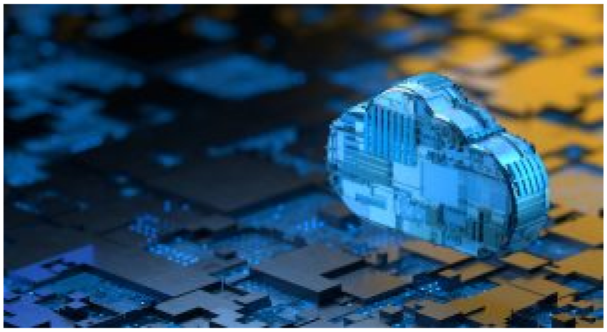
- 4b9a5de6f8d919a6c534bc8595826b9948e555b12bc0e12bbcf0099069e7df90
- 4d8472f0f60d433ffa8e90cc42f642dcb6509166cfff94472a3c1d7dcc814227
- 5ca2004cfd2b3080ac4958185323573a391dafa75f77246a00f7d0f3b42a4ca3
- 5f54177a293f9678797e831e76fd0336b0c3a4154dd0b2175f46c5a6f5782e24
- 7a502695e1cab885aee1a452cd29ce67bb1a92b37eed53d4f2f77de0ab93df9b
- 64d8bd033b4fc7e4f7fd747b2e35bce83527aa5d6396aab49c37f1ac238af4bd
- 97bd1c98ddf5b59a765ba662d72e933baab0a3310c4cdbc50791a9fe9881c775
- 268a98f359f2d56497be63a31b172bfbdc599316fb7dec086a937765af42176f
- 690d658acb9022765e1cf034306a1547847ca4adc0d48ac8a9bbdf1e6351c0f7
- 75259246f2b9f2d5b1da9e35cab254f71d82169809e5793ee9c0523f6fc19e4b
- a5cbead4c9868f83dd9b4dc49ca6baedffc841772e081a4334efc005d3a87314
- c75f99732d4e4a3ec8c19674e99d14722d8909c82830cd5ad399ce6695856666

Domains:

http[://]hw.sdk.functionads.com:8100

McAfee Labs Threat Research Team
McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs



Technical Support Scams – What to look out for

Authored by Oliver Devane Technical Support Scams have been targeting computer users for many years. Their goal...

Aug 02, 2022 | 10 MIN READ

Rise of LNK (Shortcut files) Malware

Authored by Lakshya Mathur An LNK file is a Windows Shortcut that serves as a pointer to...

Jun 21, 2022 | 6 MIN READ

Instagram credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

Jun 10, 2022 | 6 MIN READ

Instagram credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

Jun 10, 2022 | 4 MIN READ

Phishing Campaigns featuring Ursnif Trojan on the Rise

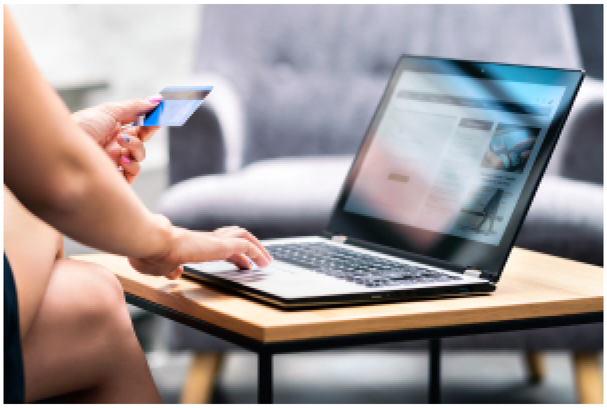
Authored by Jyothi Naveen and Kiran Raj McAfee Labs have been observing a spike in phishing campaigns...

Jun 07, 2022 | 6 MIN READ

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 25, 2022 | 4 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole   Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ