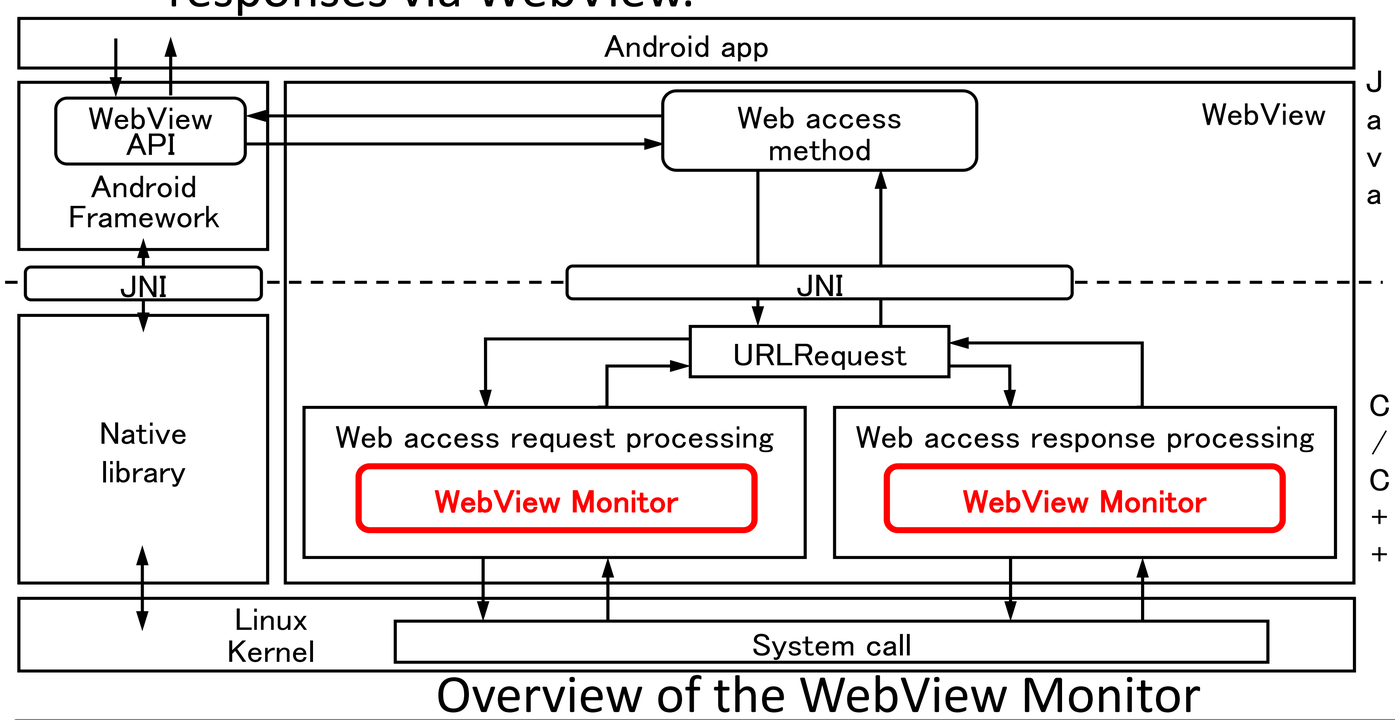
Threat Analysis of Fake Virus Alerts by Using Web Access Monitoring Mechanism for Android WebView

Rintaro Orito, Koki Riho, Yuta Imamura, Masaya Sato, Toshihiro Yamauchi (Okayama University)

1. Introduction

- Mobile web browsers are vulnerable to fake virus alerts and phishing scams.
- When analyzing web access, the following challenges are face.
  1. Identifying Android apps for analysis.
  2. Monitoring encrypted HTTP requests and responses via WebView.



Overview of the WebView Monitor

2. WebView Monitor

- WebView Monitor was proposed to gather data and analyze web access via WebView.
- WebView Monitor sends and receives data of HTTP/1,HTTP/1.1, SPDY, and HTTP/2.
- WebView Moniter has the following advantages.
  (1) WebView Monitor can monitor web access via WebView.
  (2) WebView Monitor can acquire the package name of the Android app.
  (3) WebView Monitor can acquire HTTP messages encrypted by HTTPS as plain text.

Information acquired by the WebView Monitor

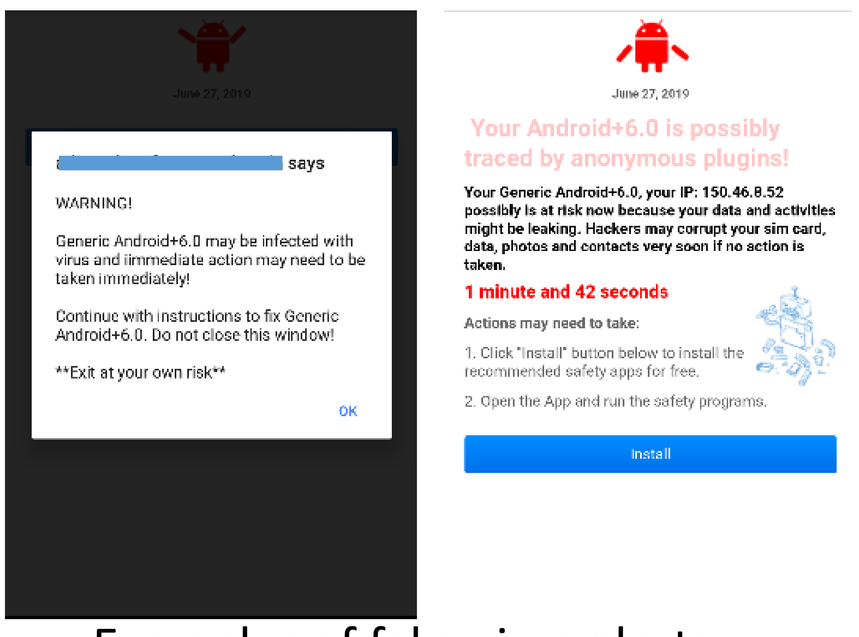
Information on web access content	● HTTP request ● HTTP response
Information on web access destination	● URL ● IP address ● Port number
Information on Android app	● Android app package name

3. Threat Analysis of Fake Virus Alert

```
&geo='JP'
&geocode='Japan'
&isp='Research Organization of Information and Systems'
&states='Okayama'
&city='Okayama'
&brand='Generic'
&browser='Chrome Mobile+'
&os='Android+6.0'
```

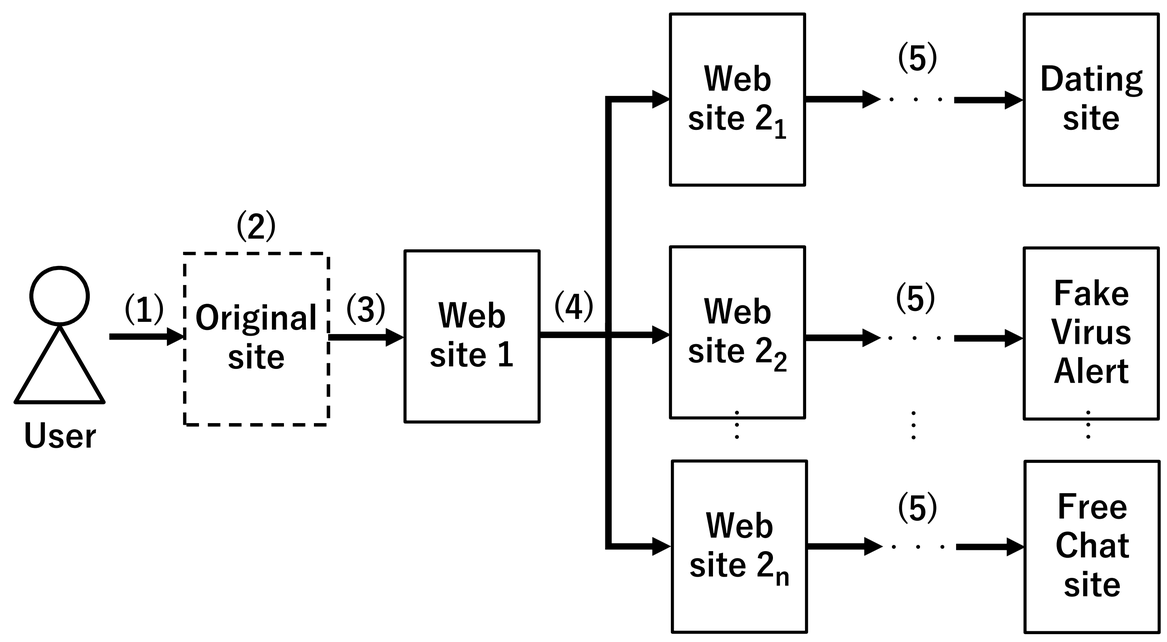
Information used for displaying a fake virus alert

- WebView Monitor revealed a JavaScript code that acquires the user information.



Examples of fake virus alerts

- Fake virus alert attempts to make a user install a suspicious app.
- These fake virus alerts are generated using the acquired user information.



Redirection flow of a fake virus alert

(1) Visiting the original website of redirection.
(2) Tapping anywhere on the screen.
(3) Redirecting to website 1.
(4) Redirecting to website 2. This redirection uses JavaScript code “window.location.replace”.
(5) Redirecting to the website that displays the fake virus alert or other unwanted website.

- JavaScript code of Website 1 creates a URL with the specified URL and a randomly created string.
  ⇒ We suppose that this is a countermeasure against URL blacklists of security tools.

4. Conclusions

- The WebView Monitor can be used to monitor web access of HTTP/1,HTTP/1.1, SPDY, and HTTP/2.
- We showed that the overhead of the WebView Monitor is reasonable.
- In future work, we will consider countermeasures against fake virus alerts based on the results of this study.

Acknowledgement : Part of this research result is obtained by contract research “WarpDrive” of research institute NICT(National Institute of Information and Communications Technology).