APJ 6 (4):12-24, Winter 2025

Arman Process Journal (APJ)

Quarterly Journal of ICT APJ

License Number: 87090

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Detect Redirect to the Malicious Web-Sites in ANDROID Devices

S. M. Hashimi [1]

[1] Department of Computer Engineering , Institute of Higher Education , Qazvin , Iran

RESEARCH PAPER

Received: 2025-8-14
Accepted: 2026-2-17

KEYWORDS:
ANDROID,
Redirect,
malicious web-sites,
Detecting

[1]Corresponding author:
[1]
hashemi2138@yahoo.com

ABSTRACT

Background and Objectives: Website clicks that redirect Android phone users to malicious websites with fake virus warnings or phishing attacks are increasing exponentially. Although a Uniform Resource Locator (URL) blacklist is considered as a suitable countermeasure for such attacks, it is difficult to efficiently identify malicious websites. To the best of our knowledge, no research has focused on detecting attacks that redirect Android phone users to malicious websites. Therefore, we propose a redirection detection method that focuses on the URL bar change interval of the Android-based Google Chrome browser.

Methods: The proposed method, which can be easily installed as an Android application, uses the Android Accessibility Service to detect unwanted redirects to malicious websites without collecting information about these websites in advance. This paper describes the details of the design, implementation, and evaluation results of the proposed application on a real Android device. We set threshold values for the number of times the URL bar changes and the elapsed time to detect redirects to malicious websites for the proposed method.

Finding: This work has two advantges. At the first, the presented lgorithm is simpler than other ways. The second, the algorithm is more effective than others. Based on the results, we investigated the causes of false positive detections of redirects to safe websites and proposed solutions to manage them. We also present threshold values that can minimize the false positive and negative rates, as well as the detection accuracy of the proposed method based on these threshold values. In addition, we present evaluation results based on access reports of real users participating in the WarpDrive project experiment, which show that the proposed method minimizes false positives and successfully detects most redirects to malicious websites.

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۴، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

شناسایی هدایت مجدد به وب سایتهای مخرب در وسایل اندروید

سید محمود هاشمی

گروه کامپیوتر، دانشکده مهندسی، موسسه آموزش عالی کار، قزوین، ایران

چکیده

مقاله پژوهشی

پیشینه و اهداف: کلیک‌های وب‌سایت که کاربران تلفن‌های اندروید را به وب‌سایت‌های مخرب با هشدارهای جعلی ویروس یا حملات فیشینگ هدایت می‌کنند، به صورت تصاعدی در حال افزایش هستند. اگرچه یک لیست سیاه مکان‌یاب منبع یکنواخت (URL) به عنوان یک اقدام متقابل مناسب برای چنین حملاتی در نظر گرفته می‌شود، اما شناسایی کارآمد وب‌سایت‌های مخرب دشوار است. تا آنجا که ما می‌دانیم، هیچ تحقیقی بر تشخیص حملاتی که کاربران تلفن‌های اندروید را به وب‌سایت‌های مخرب هدایت می‌کنند، متمرکز نشده است. بنابراین، ما یک روش تشخیص تغییر مسیر را پیشنهاد می‌کنیم که بر فاصله زمانی تغییر نوار URL مرورگر گوگل کروم مبتنی بر اندروید تمرکز دارد.

روشها: روش پیشنهادی، که به راحتی به عنوان یک برنامه اندروید قابل نصب است، از سرویس دسترسی اندروید برای شناسایی تغییر مسیرهای ناخواسته به وب‌سایت‌های مخرب بدون جمع‌آوری اطلاعات در مورد این وب‌سایت‌ها از قبل استفاده می‌کند. این مقاله جزئیات طراحی، پیاده‌سازی و نتایج ارزیابی برنامه پیشنهادی را بر روی یک دستگاه اندروید واقعی شرح می‌دهد .ما مقادیر آستانه برای تعداد دفعات تغییر نوار URL و زمان سپری شده برای تعیین تغییر مسیرها به وب‌سایت‌های مخرب را برای روش پیشنهادی تعیین کردیم.

یافته ها: مقاله دارای دو مزیت عمده است. اولا الگوریتم ارایه شده در این مقاله بسیار ساده تر از روششهای قبلی است و ثانیا روش اراه شده بسیار کاراتر است. بر اساس نتایج، ما علل تشخیص‌های مثبت کاذبِ تغییر مسیرها به وب‌سایت‌های بی‌خطر را بررسی کردیم و راه‌حل‌هایی برای مدیریت آنها ارائه دادیم. همچنین مقادیر آستانه‌ای که می‌توانند نرخ‌های مثبت و منفی کاذب را به حداقل برسانند، و همچنین دقت تشخیص روش پیشنهادی بر اساس این مقادیر آستانه را ارائه می‌دهیم. علاوه بر این، نتایج ارزیابی‌ها را بر اساس گزارش‌های دسترسی کاربران واقعی شرکت‌کننده در آزمایش پروژه WarpDrive ارائه می‌دهیم که نشان می‌دهد روش پیشنهادی، موارد مثبت کاذب را به حداقل می‌رساند و اکثر تغییر مسیرها به وب‌سایت‌های مخرب را با موفقیت تشخیص می‌دهد.

واژگان کلیدی:
اندروید،
هدایت مجدد،
وب سایت بدخواه،
تشخیص.

مقدمه

با افزایش محبوبیت دستگاه‌های تلفن همراه، حملاتی که این دستگاه‌ها را هدف قرار می‌دهند، به طور فزاینده‌ای جدی می‌شوند. در سه‌ماهه چهارم سال ۲۰۲۳، دستگاه‌های تلفن همراه تقریباً ٪۵۴٫۶۷ از ترافیک وب جهانی را ایجاد کردند [۱] و این به طور مداوم در حال افزایش است. مک‌آفی گزارش داده است که حملاتی که دستگاه‌های تلفن همراه را هدف قرار می‌دهند، پیچیده‌تر می‌شوند و انتظار می‌رود به طور مداوم افزایش یابند [۲]. دستگاه‌های اندروید رایج‌ترین اهداف حملات دستگاه‌های تلفن همراه هستند، در درجه اول به این دلیل که توسط بخش بیشتری از کاربران استفاده می‌شوند. در فوریه ۲۰۲۴، ٪۷۱٫۴۳ از دستگاه‌های تلفن همراه مورد استفاده در سراسر جهان مبتنی بر اندروید بودند [۳]. علاوه بر این، توزیع برنامه‌های مخرب در اندروید برای مهاجمان آسان‌تر است زیرا برنامه‌های iOS (اپل) توسط اپل به دقت بررسی می‌شوند، در حالی که برنامه‌های اندروید را می‌توان از طریق وب‌سایت‌های خارجی یا فروشگاه‌های برنامه‌های شخصی و بدون بررسی توسط گوگل توزیع کرد. یکی از این حملات شامل تغییر مسیر به وب‌سایت‌های مخرب است و با دسترسی کاربر به یک وب‌سایت منبع یا کلیک روی پیوندی در آن آغاز می‌شود. هدف این حملات، کسب درآمد از تبلیغات، جمع‌آوری اطلاعات شخصی یا نصب برنامه‌های مخرب با هدایت کاربران به وب‌سایت‌هایی است که هشدارها یا نظرسنجی‌های دروغین را نمایش می‌دهند. دلیل این امر این است که برخلاف سیستم‌عامل‌های رایانه‌های شخصی، دستگاه‌های تلفن همراه به کاربران اجازه نصب برنامه‌ها را بدون اجازه آنها نمی‌دهند. در واقع، گزارش شده است که یک کمپین جمع‌آوری اعتبارنامه فیس‌بوک در مقیاس بزرگ از یک زنجیره تغییر مسیر استفاده کرده است [۴]. یک اقدام متقابل (CM) برای چنین حملاتی، استفاده از لیست سیاهی از مکان‌یاب‌های منابع یکسان (URL) و دامنه‌ها است. با این حال، جلوگیری از انتقال به وب‌سایت‌های مخرب دشوار است.

استفاده از این تکنیک [۵]، [۶] به این دلیل که وب‌سایت‌های مخرب زیادی وجود دارند و URLها و نام‌های دامنه آنها با تغییرات کوتاه‌مدت مشخص می‌شوند [۷] غیر کاربردی است. علاوه بر این CM، برخی مطالعات با هدف شناسایی وب‌سایت‌های مخرب با استفاده از تکنیک‌های دیگر انجام شده‌اند. لی و همکارانش [۸] روشی را برای تشخیص تزریق اسکریپت تغییر مسیر با استفاده از تحلیل تفاضلی پیشنهاد کردند. آنها کدهای جاوا اسکریپت (JS) مخرب را استخراج کرده و با استفاده از تفاوت بین کتابخانه‌های JS مخرب و قانونی، بر اساس این مشاهده که فایل‌های JS که بیشتر مورد حمله قرار می‌گیرند، کتابخانه‌های JS شخصی هستند که نسخه‌های سالم آنها به صورت عمومی در دسترس است، امضاهایی ایجاد کردند. با این حال، اعمال روش‌هایی که سیستم عامل اندروید را هدف قرار نمی‌دهند، برای دستگاه‌های اندروید دشوار است، زیرا برخلاف سیستم‌های عامل دسکتاپ، نظارت بر ارتباطات مرورگر وب در دستگاه‌های اندروید دشوار است و در نتیجه اقدامات امنیتی قابل اجرا را محدود می‌کند.

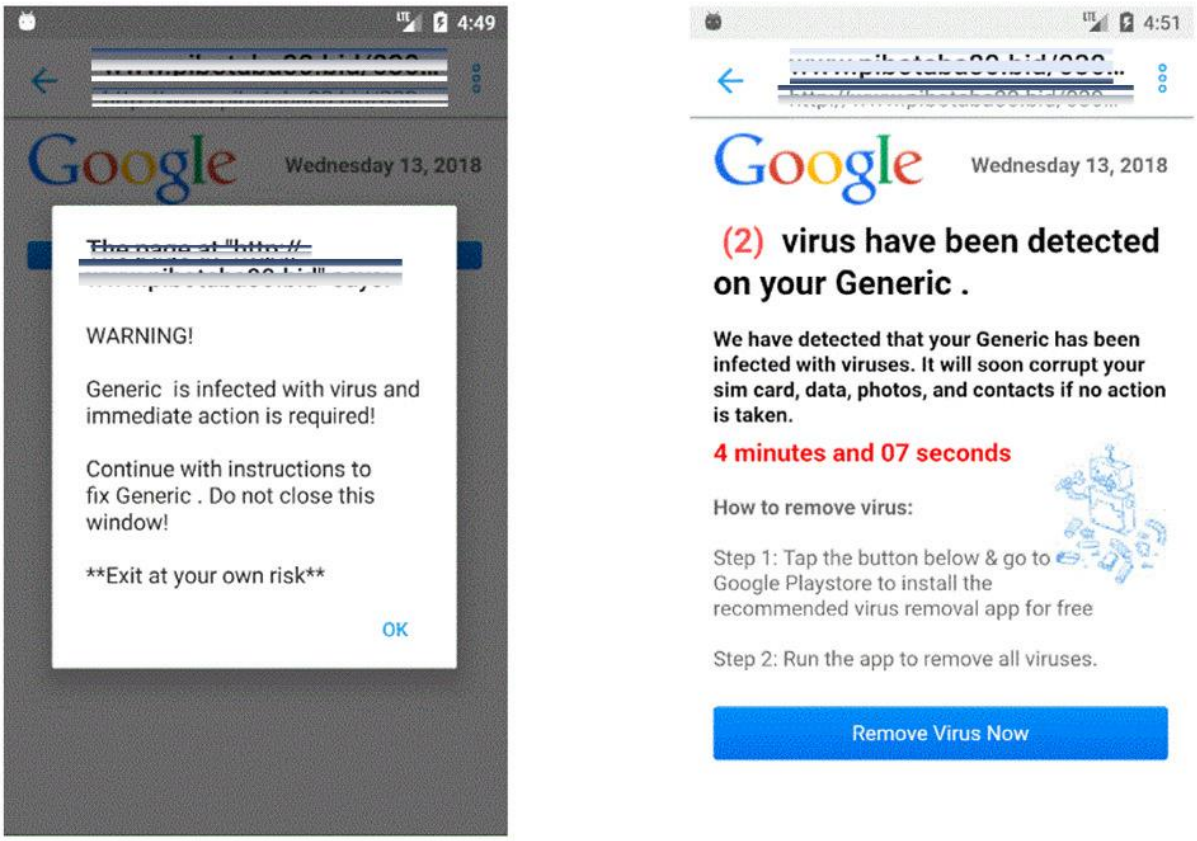
بنابراین، ما روشی را برای تشخیص تغییر مسیرها به وب‌سایت‌های مخرب در دستگاه‌های اندروید با استفاده از یک سرویس دسترسی پیشنهاد می‌کنیم. این روش می‌تواند تنها با نظارت بر فاصله زمانی تعویض نوار آدرس در مرورگر، بدون جمع‌آوری اطلاعات در مورد وب‌سایت‌های مخرب از قبل، تغییر مسیرها به وب‌سایت‌های مخرب را تشخیص دهد. علاوه بر این، از آنجا که به عنوان یک برنامه اندروید پیاده‌سازی شده است، همه کاربران اندروید می‌توانند به راحتی آن را بپذیرند. علاوه بر این، با به حداقل رساندن نتایج مثبت کاذب تغییر مسیرهای وب‌سایت‌های بی‌خطر، قابلیت استفاده را بهبود می‌بخشد. به طور خاص، تغییر مسیرهای وب‌سایت ناشی از عملیات کاربر، مانند لمس لینک یا عملیات "برگشت" را تشخیص می‌دهد و بر اساس این واقعیت که کاربران به طور خودکار از طریق چندین تغییر مسیر متوالی به وب‌سایت‌های مخرب هدایت می‌شوند، تعیین می‌کند که آنها تغییر مسیر به وب‌سایت‌های مخرب نیستند. با این حال، تغییر مسیرهای متوالی صفحه حتی ممکن است در وب‌سایت‌های بی‌خطر در حین عملیات کاربر، مانند صفحات احراز هویت، رخ دهد. بنابراین، روش پیشنهادی، تشخیص‌های تغییر مسیر مثبت کاذب و منفی کاذب را شناسایی می‌کند. این مطالعه علل مثبت کاذب را تجزیه و تحلیل کرده و روشی برای به حداقل رساندن آنها پیشنهاد می‌دهد. برنامه پیشنهادی با نصب چندین کاربر واقعی اندروید و دریافت داده‌های استفاده آنها ارزیابی شد. نتایج نشان داد که می‌تواند کاربران را از وب‌سایت‌های مخرب محافظت کند. داده‌ها از طریق یک سیستم مشاهده حمله مبتنی بر وب مشارکتی کاربر برای تلفن‌های هوشمند از پروژه WarpDrive9 جمع‌آوری شدند.

موارد اصلی این مطالعه به شرح زیر است:

- این مقاله روش جدیدی را برای تشخیص حملاتی پیشنهاد می‌کند که کاربران اندروید را بر اساس فاصله زمانی تعویض صفحه وب به وب‌سایت‌های مخرب هدایت می‌کنند. این روش را می‌توان به راحتی در دستگاه‌های اندروید به عنوان یک سرویس دسترسی، که

یک ویژگی استاندارد اندروید است که برای نظارت بر مرورگرها استفاده می‌شود، پیاده‌سازی کرد.

روش پیشنهادی می‌تواند وب‌سایت‌های مخرب را بدون جمع‌آوری اطلاعات آنها از قبل شناسایی کند، زیرا فقط بر فاصله زمانی تعویض صفحات وب تمرکز دارد. بنابراین، می‌تواند به طور مداوم وب‌سایت‌های مضری را که URLها و دامنه‌های آنها به سرعت تغییر می‌کنند و بنابراین در لیست سیاه قرار نمی‌گیرند، شناسایی کند. شکل ۱. نمونه‌ای از صفحه هشدار کاذب در یک وب‌سایت مخرب.



شکل ۱. نمونه هایی از سایتهای مخرب

روش پیشنهادی نوار URL را رصد می‌کند و همزمان اقدامات کاربر، مانند ضربه زدن، را شناسایی می‌کند تا بین اقدامات آنها در وب‌سایت‌های بی‌خطر و تغییر مسیرهای متوالی به وب‌سایت‌های مخرب تمایز قائل شود. در نتیجه، تشخیص‌های مثبت کاذب تغییر مسیرها به وب‌سایت‌های بی‌خطر را سرکوب می‌کند و می‌تواند برای کاربران بسیار مفید باشد. اثربخشی روش پیشنهادی با استفاده از داده‌های بسیاری از کاربران واقعی که از آن استفاده کرده‌اند ارزیابی شد و تأیید شد که با موفقیت آنها را از وب‌سایت‌های مضر محافظت می‌کند.

یک حمله رایج که کاربران اندروید را هدف قرار می‌دهد، شامل هدایت ناخواسته آنها به وب‌سایت‌های مخرب است. مهاجمان، کاربرانی را که به سایت‌های ویدیویی رایگان، سایت‌های کمیک و غیره دسترسی دارند، به وب‌سایت‌های مخرب هدایت می‌کنند و در آنجا از روش‌های مختلفی برای فریب آنها جهت دستیابی به اهداف زیر استفاده می‌کنند:

- کسب درآمد از تبلیغات.
- جمع‌آوری اطلاعات شخصی.
- وادار کردن آنها به ثبت‌نام برای خدمات پولی.
- نصب بدافزار.

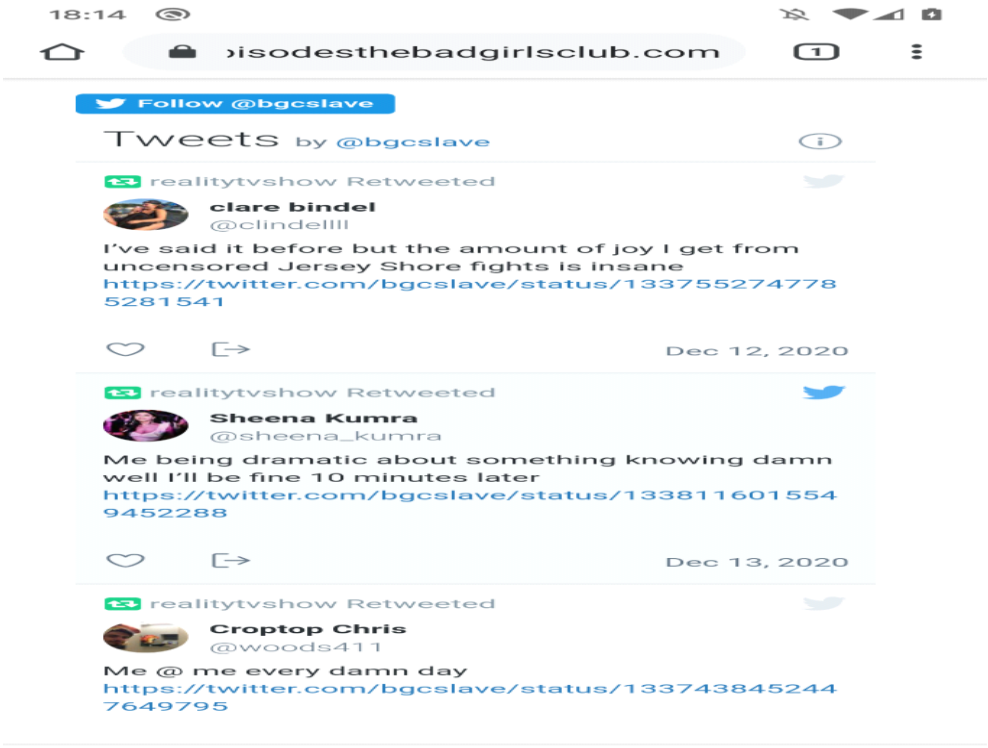
این بخش تکنیک‌های مورد استفاده مهاجمان برای فریب کاربران را توضیح می‌دهد. نمونه‌ای از یک وب‌سایت مخرب که یک صفحه هشدار کاذب را نمایش می‌دهد، در شکل ۱ نشان داده شده است

که هدف آن ترغیب کاربران به نصب یک برنامه آنتی‌ویروس جعلی است. این هشدار جعلی، لوگوی گوگل و اطلاعات دستگاه کاربر را با هدف ایجاد اعتماد آنها نمایش می‌دهد. این وب‌سایت‌ها همچنین ممکن است ویبره و صداهای هشدار ایجاد کنند تا کاربران را ناراحت کنند و آنها را به این باور برسانند که تلفن‌های هوشمندشان به بدافزار آلوده شده است.

تغییر مسیر به وب‌سایت‌های مخرب برخلاف میل کاربر می‌تواند به صورت خودکار رخ دهد یا توسط عملیاتی مانند لمس یک نقطه دلخواه روی صفحه نمایش ایجاد شود. شکل ۲ نمونه‌ای از یک وب‌سایت با منبع تغییر مسیر را نشان می‌دهد. وقتی کاربر روی هر نقطه‌ای از این صفحه (داخل خط چین) ضربه می‌زند، یک تغییر مسیر ناخواسته رخ می‌دهد. کارهای زیر در عملیات پیوند با استفاده از یک پنل لمسی، مانند تلفن هوشمند [۱۰]، تجمیع می‌شوند:

- عنصر پیوندی را که کاربر می‌خواهد لمس کند، پیدا کنید.
- عنصر پیوند را برای انتقال به مقصد پیوند لمس کنید.

از آنجایی که وب‌سایت منبع نشان داده شده در شکل ۲ حاوی یک پیوند شفاف به یک وب‌سایت مخرب است، کاربر نمی‌تواند عنصر پیوند را تشخیص دهد (یعنی عملیات ۱ رضایت‌بخش نیست). لمس چنین پیوندهای ناشناخته‌ای، آنها را برخلاف هدفشان به یک وب‌سایت مخرب هدایت می‌کند.



شکل ۲. نمونه ای از یک وب سایت با هدایت مجدد

یک مطالعه قبلی [۱۱] ویژگی‌های تغییر مسیرها به وب‌سایت‌های مخرب را با استفاده از وب‌سایت‌های منبع کشف شده از طریق جستجوهای وب، توییتر و فیس‌بوک تجزیه و تحلیل کرد و جریان تغییر مسیرها از منبع به وب‌سایت‌های مخرب را نشان داد. ویژگی‌های انتقال به وب‌سایت‌های مخرب را می‌توان به شرح زیر خلاصه کرد:

۱. انتقال از طریق دو یا چند (اغلب سه یا بیشتر) وب‌سایت.
۲. چندین تغییر مسیر در دوره‌های کوتاه.
۳. ایجاد URL های مختلف برای هر دسترسی.
۴. عدم ثبت سابقه مرور.
۵. تفاوت در وقوع تغییر مسیر بر اساس وجود یا عدم وجود کوکی‌ها.
۶. استفاده از انواع مختلف کدهای تغییر مسیر.

CM های فعلی در برابر تغییر مسیر به وب‌سایت‌های مخرب شامل لیست سیاه و تشخیص کدهای JS مخرب هستند. اگرچه لیست سیاه در بسیاری از برنامه‌های امنیتی اندروید استفاده می‌شود، اما نمی‌تواند وب‌سایت‌های مخرب را به طور موثر تشخیص دهد [۵]، [۶] زیرا URL های وب‌سایت‌های مخرب با هر دسترسی تغییر

می‌کنند، همانطور که در بخش II-C توضیح داده شده است. علاوه بر این، اعمال این روش در دستگاه‌های اندروید دشوار است زیرا برنامه‌های امنیتی اندروید نمی‌توانند محتوای ارتباطات مرورگر وب را رصد کنند و این نوع حمله چندین کد JS را مبهم می‌کند. بنابراین، شناسایی کد JS خاصی که باعث تغییر مسیر می‌شود دشوار است. علاوه بر این، این تکنیک نمی‌تواند بین تغییر مسیرها به وب‌سایت‌های مخرب و بی‌خطر تمایز قائل شود.

تحقیقات مشابه

مرجع [۱۲] روشی را برای تشخیص دسترسی به وب‌سایت‌های مخرب بر اساس اسکرین‌شات‌های وب‌سایت‌های مشاهده‌شده توسط کاربران ارائه داده است. این روش از یک CNN سطح کاراکتری، که نوعی شبکه عصبی عمیق است، برای یادگیری و طبقه‌بندی اسکرین‌شات‌های وب‌سایت استفاده کرد. با این حال، این روش بر سیستم عامل اندروید تمرکز نداشت و نیاز به یادگیری قبلی با جمع‌آوری اطلاعات در مورد وب‌سایت‌های مخرب داشت. برخی مطالعات نیز بر ویژگی‌های تغییر مسیر به وب‌سایت‌های مخرب تمرکز کرده‌اند [۱۳]، [۱۴]. در [۱۳]، از یک کلاینت بسیار تعاملی برای جمع‌آوری خودکار اطلاعات قابل توجهی در مورد تغییر مسیرها به وب‌سایت‌های مخرب در طول حملات Drive-by Download استفاده شده است. همچنین تغییر مسیرها به وب‌سایت‌های مخرب را بر اساس شباهت ساختاری اطلاعات تغییر مسیر جمع‌آوری‌شده شناسایی کرد. در [۱۴]، اطلاعات مربوط به تغییر مسیرها به وب‌سایت‌های مخرب از طیف وسیعی از کاربران جمع‌آوری شد. از نتایج جمع‌آوری‌شده، نموداری که جریان تغییر مسیرها به وب‌سایت‌های مخرب را نشان می‌دهد، ایجاد شده و بر اساس آن، تغییر مسیرها به وب‌سایت‌های مخرب شناسایی شدند. اگرچه این مطالعات [۱۳]، [۱۴] بر روی چندین تغییر مسیر به وب‌سایت‌های مخرب تمرکز داشتند، اما با روش پیشنهادی متفاوت بودند، زیرا سیستم عامل اندروید را هدف قرار نمی‌دادند و از قبل به اطلاعات مربوط به وب‌سایت‌های مخرب نیاز داشتند.

این مطالعه با هدف توسعه روشی برای اطلاع‌رسانی به کاربران اندروید مبنی بر دسترسی به وب‌سایت‌های مخرب انجام شده است. روش پیشنهادی، تغییر مسیر به وب‌سایت‌های مخرب را بدون جمع‌آوری اطلاعات در مورد وب‌سایت مخرب یا تجزیه و تحلیل کد HTML یا JS در زمان تغییر مسیر، تشخیص می‌دهد.

این مطالعه بر ویژگی‌های ۱ و ۲ شرح داده شده در بخش قبلی تمرکز دارد که در آن چندین تغییر مسیر در یک دوره کوتاه رخ می‌دهد. این ویژگی‌ها مستقل از نوع کد تغییر مسیر مورد استفاده هستند که یک ویژگی رایج در بسیاری از تغییر مسیرهای وب‌سایت‌های مخرب است. روش پیشنهادی با شناسایی ویژگی‌های تغییر مسیرهای متوالی به چنین وب‌سایت‌هایی بدون نظارت بر محتوای ارتباط مرورگر وب، مزیت تشخیص تغییر مسیرهای ناخواسته به وب‌سایت‌های مخرب را ارائه می‌دهد.

بخش‌های زیر طراحی روش پیشنهادی را ارائه می‌دهند. این مطالعه مرورگر گوگل کروم را در دستگاه‌های اندروید به عنوان هدف نظارت در نظر گرفته است.

ما می‌خواستیم کاربران بتوانند به راحتی از روش پیشنهادی در تلفن‌های هوشمند اندرویدی خود، مشابه هر برنامه دیگری، استفاده کنند و بنابراین، آن را به عنوان یک برنامه اندرویدی پیاده‌سازی کردیم. اگرچه هسته لینوکس یا چارچوب اندروید، که اساس اندروید است، قابلیت اضافه کردن یک تابع برای نظارت بر ارتباطات وب را ارائه می‌دهد، ما از این روش استفاده نکردیم زیرا استفاده از روش پیشنهادی را در تلفن‌های هوشمند برای کاربران عادی دشوار می‌کرد. اصول طراحی روش پیشنهادی را می‌توان به شرح زیر خلاصه کرد:

نظارت بر دسترسی به وب توسط مرورگرهای وب در برنامه‌های اندروید: یک روش برای برنامه‌های اندروید برای نظارت بر ارتباطات یک مرورگر وب، استفاده از یک شبکه خصوصی مجازی (VPN) است [۱۵]. با این حال، این روش مشکلات زیر را برای کاربران عادی ایجاد می‌کند:

۱. ساخت و مدیریت یک سرور اختصاصی VPN پرهزینه است. استفاده از VPN می‌تواند سرعت ارتباط را به میزان قابل توجهی کاهش دهد. بنابراین، روش پیشنهادی ارتباطات دسترسی به وب را رصد نمی‌کند و لازم است دسترسی به وب توسط مرورگرهای وب از طریق برنامه‌های دیگر رصد شود.

۲. توانایی تشخیص تغییر مسیرها به وب‌سایت‌های مخرب بدون جمع‌آوری اطلاعات آنها از قبل: تغییر مسیرها به وب‌سایت‌های مخرب باعث تغییر مسیر چندگانه در یک دوره کوتاه می‌شوند. ما از ویژگی‌های این تغییر مسیرها برای تشخیص آنها استفاده کردیم.

۳. کاهش نرخ مثبت کاذب تشخیص تغییر مسیر در وب‌سایت‌های بی‌خطر: تغییر مسیرها به وب‌سایت‌های مخرب ممکن است همان ویژگی‌های وب‌سایت‌های بی‌خطر را داشته باشند، که ممکن است باعث شود روش پیشنهادی تغییر مسیرها به وب‌سایت‌های بی‌خطر را به اشتباه مانند

وب‌سایت‌های مخرب تشخیص دهد. از آنجا که فراوانی بالای مثبت‌های کاذب ممکن است راحتی و عملکرد روش پیشنهادی را کاهش دهد، لازم است آنها را به حداقل برسانیم.

شکل ۴ فرآیند روش پیشنهادی را نشان می‌دهد. پس از نصب برنامه، کاربر باید سرویس دسترسی آن را در تنظیمات دستگاه خود فعال کند. هنگامی که کاربر این تنظیم را فعال می‌کند و از یک مرورگر وب استفاده می‌کند، برنامه به شرح زیر عمل می‌کند:

a) رویدادهای ``TYPE_WINDOW_CONTENT_CHANGED`` یا ``CONTENT_CHANGE_TYPE_TEXT`` رصد می‌شوند.

b) هنگامی که یکی از این رویدادها رخ می‌دهد، برنامه تعیین می‌کند که آیا در نوار URL مرورگر وب رخ داده است یا خیر.

c) اگر رویداد در نوار URL رخ دهد، یک مهر زمانی از زمان وقوع آن به دست می‌آید.

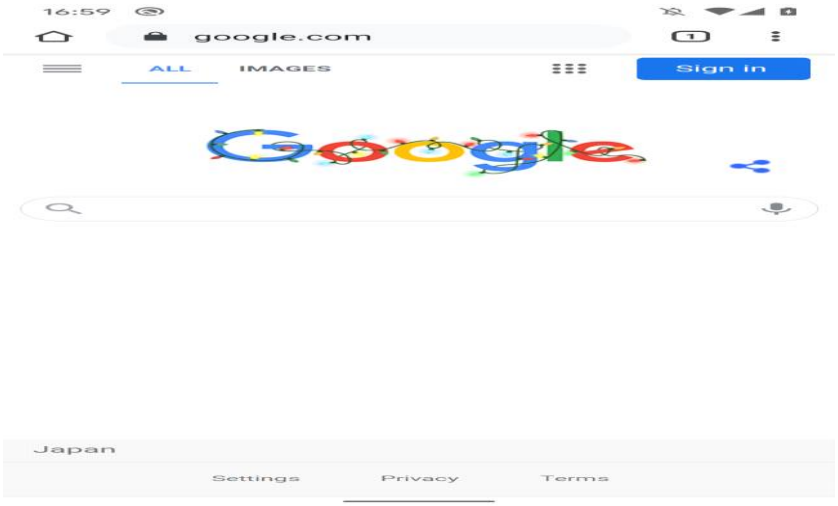
d) زمان سپری شده از مهر زمانی به دست آمده محاسبه می‌شود.

e) اگر زمان سپری شده کوتاه‌تر از Threshold_2 باشد، به کاربر اطلاع داده می‌شود که یک تغییر مسیر به یک وب‌سایت مخرب شناسایی شده است.

روش پیشنهادی از یک سرویس دسترسی [۱۶] برای نظارت بر دسترسی مرورگر وب و تغییرات در نوار آدرس آن استفاده می‌کند. سرویس دسترسی می‌تواند تغییرات در صفحه نمایش دستگاه اندروید و عملیات کاربر (رویدادها) را نظارت کند. همچنین به کاربران در استفاده از یک برنامه بر اساس اطلاعات رویدادهای به دست آمده کمک می‌کند. شکل۳ یک صفحه مرورگر را نشان می‌دهد که صفحه اصلی جستجوی گوگل را در یک دستگاه اندروید و نماهایی که می‌توانند توسط سرویس‌های دسترسی نظارت شوند، نمایش می‌دهد. حاشیه صفحه اندروید، کل نما، شامل نوار آدرس، کادر جستجو و دکمه «ورود» را نشان می‌دهد. نما، رابط کاربری است که صفحه برنامه اندروید را تشکیل می‌دهد. سرویس‌های دسترسی می‌توانند تغییرات در نما و ضربه‌های کاربران را نظارت کنند. روش پیشنهادی، نمای نوار آدرس مرورگر وب را با استفاده از سرویس دسترسی نظارت می‌کند تا تغییرات در متن آن را بر اساس تغییرات در وب‌سایت نمایش داده شده شناسایی کند. تغییرات در متن نوار آدرس اینترنتی (URL Bar) می‌تواند توسط سرویس دسترسی در صورت وقوع رویدادهای زیر، پایش شود:

- TYPE_WINDOW_CONTENT_CHANGED
- CONTENT_CHANGE_TYPE_TEXT

روش پیشنهادی، وقوع این رویدادها را پایش می‌کند. سرویس دسترسی می‌تواند اطلاعاتی در مورد یک رویداد پایش‌شده، که یک ویژگی نامیده می‌شود، به دست آورد. روش پیشنهادی، شناسه منبع (Resource ID) نمای (view) که یک رویداد در آن رخ می‌دهد را به دست می‌آورد، که به آن اجازه می‌دهد بررسی کند که آیا یک رویداد پایش‌شده در نوار آدرس اینترنتی (URL Bar) رخ می‌دهد یا خیر. شناسه منبع شامل نام بسته برنامه‌ای است که شامل نما و شناسه‌های آن است. با به دست آوردن شناسه منبع، نمای (view) که رویداد در آن رخ می‌دهد، قابل شناسایی است. بنابراین، هنگامی که رویدادهای فوق‌الذکر در نوار آدرس اینترنتی (URL Bar) رخ می‌دهند، روش پیشنهادی تعیین می‌کند که وب‌سایت نمایش داده شده توسط مرورگر به دلیل دسترسی به وب تغییر کرده است.



شکل ۳. مثالی از سایت نظارت شده

روش پیشنهادی تعیین می‌کند که تغییر مسیر به یک وب‌سایت مخرب زمانی رخ داده است که نوار آدرس (URL Bar) در یک دوره کوتاه به طور مداوم تغییر کند. این امر بر اساس این ویژگی است که تغییر مسیر به یک وب‌سایت مخرب می‌تواند باعث تغییر مسیرهای متعدد در یک دوره کوتاه شود. بر اساس این ویژگی، تغییر مسیرها به وب‌سایت‌های مخرب بر اساس رویدادهای `TY PE_WINDOW_CONTENT_CHANGED` یا `CONTENT_CHA NGE_TYPE_TEXT` شناسایی می‌شوند که نشان می‌دهد محتوای نوار آدرس (URL Bar) تغییر کرده است. بر این اساس، روش پیشنهادی تغییر مسیرها به وب‌سایت‌های مخرب را با استفاده از آستانه‌های زیر تشخیص می‌دهد:

آستانه ۱: تعداد تغییر مسیرها در نوار آدرس برای محاسبه زمان سپری شده.

آستانه ۲: زمان سپری شده برای شناسایی تغییر مسیرها به وب‌سایت‌های مخرب.

شکل ۶ نشان می‌دهد که چگونه روش پیشنهادی تغییر مسیرها به وب‌سایت‌های مخرب را تشخیص می‌دهد. این روش زمان فعلی هر دسترسی به وب را دریافت کرده و زمان سپری شده را بر اساس زمان آخرین دسترسی به وب و چندین دسترسی قبلی به وب محاسبه می‌کند.

Threshold_1 زمان سپری شده از دسترسی‌های قبلی به وب را که باید در این محاسبه استفاده شوند، تعیین می‌کند. اگر زمان سپری شده کوتاه‌تر از Threshold_2 باشد، روش پیشنهادی تعیین می‌کند که تغییر مسیر به یک وب‌سایت مخرب است. شکل ۶ مثالی را نشان می‌دهد که در آن Threshold_1 روی سه تنظیم شده است.

Threshold_1 و Threshold_2 بر اساس ارزیابی با استفاده از وب‌سایت‌های واقعی سالم و مخرب تنظیم شده‌اند.

روش پیشنهادی، تغییر مسیرها به وب‌سایت‌های مخرب را بر اساس این ویژگی که وب‌سایت‌ها به طور مداوم در یک دوره کوتاه تغییر می‌کنند، تشخیص می‌دهد. با این حال، یک کاربر ممکن است در یک دوره کوتاه به یک وب‌سایت بی‌خطر نیز تغییر مسیر دهد. علاوه بر این، برخی از وب‌سایت‌های بی‌خطر ممکن است در طول احراز هویت کاربر به طور مداوم صفحات را تغییر دهند. در چنین مواردی، روش پیشنهادی ممکن است تغییر مسیرها را در وب‌سایت‌های بی‌خطر به اشتباه تشخیص دهد. بنابراین، عملیات کاربر که باعث مثبت کاذب می‌شوند، بررسی و به شرح زیر شناسایی شدند:

۱. لمس یک لینک

۲. لمس یک لینک.

فشار دادن کلید برگشت.

از لینک‌های لنگر که در همان وب‌سایت منتقل می‌شوند استفاده می‌شود.

کشیدن انگشت.

وارد کردن متن.

روش پیشنهادی با شناسایی این عملیات، تعداد تشخیص‌های تغییر مسیر مثبت کاذب به وب‌سایت‌های بی‌خطر را به حداقل می‌رساند. شکل ۷ فرآیند به کار رفته در روش پیشنهادی برای تشخیص این عملیات را نشان می‌دهد. بر اساس ویژگی‌های تغییر مسیرها به وب‌سایت‌های مخرب که در بخش II-C شرح داده شده است، موارد زیر قابل تشخیص است:

در بسیاری از موارد، چهار یا چند تغییر متوالی وب‌سایت رخ می‌دهد.

تغییر مسیر خودکار از عملیات کاربر در طول تغییر مسیرها جلوگیری می‌کند.

بر اساس این ویژگی‌ها، سه تغییر مسیر متوالی به یک وب‌سایت پس از شناسایی عملیات کاربر می‌تواند به عنوان تغییر مسیر به وب‌سایت‌های مخرب تعیین نشود. در شکل ۷، Threshold_1 روی سه تنظیم شده است. در این حالت، روش پیشنهادی، تغییر مسیر در مرحله ۵ را به عنوان تغییر مسیر به یک وب‌سایت مخرب قضاوت می‌کند، حتی اگر عملیات کاربر در وب‌سایت منبع شناسایی شود.

در ادامه، شش CM را شرح می‌دهیم که از طریق آنها روش پیشنهادی عملیات کاربر را شناسایی می‌کند.

(CM1) نام دامنه کاملاً واجد شرایط (FQDN)

لیست سفید

روش پیشنهادی با ایجاد لیست سفیدی از FQDN های وب‌سایت‌های بی‌خطر، تعداد موارد مثبت کاذب را به حداقل می‌رساند.

به طور خاص، تغییر مسیر به چنین وب‌سایت‌هایی، صرف نظر از زمان سپری شده، به عنوان تغییر مسیر به وب‌سایت‌های مخرب در نظر گرفته نمی‌شوند.

ما لیست وب‌سایت‌های رتبه ۱۵۰ در سایت‌های برتر الکسا (ژاپن) [۱۷] را در ۲۶ مه ۲۰۲۰ به دست آوردیم و یک لیست سفید از ۱۳ FQDN برای وب‌سایت‌های بی‌خطر ایجاد کردیم تا موارد مثبت کاذب را به حداقل برسانیم.

(CM2) شناسایی ضربه‌های لینک

هنگامی که کاربر روی محتوای حاوی یک لینک ضربه می‌زند، رویداد ``T YPE_VIEW_CLICKED'' یا ``TYPE_VIEW_FOCUSED'' رخ می‌دهد. این رویدادها را می‌توان از طریق سرویس دسترسی مشاهده کرد. روش پیشنهادی با مشاهده این رویدادها، لمس لینک‌ها را تعیین می‌کند. فرآیندی که هنگام تشخیص لمس لینک اجرا می‌شود در شکل ۷ نشان داده شده است.

(CM3) شناسایی عملیات "برگشت"

روش پیشنهادی، URLهای وب‌سایت‌های بازدید شده توسط کاربران در گذشته را ذخیره می‌کند. اگر URL وب‌سایتی که کاربر به آن دسترسی پیدا کرده است با یک URL ذخیره شده مطابقت داشته باشد، روش پیشنهادی تعیین می‌کند که کاربر عملیات "برگشت" را انجام داده است و آن را مطابق شکل ۷ پردازش می‌کند.

روش پیشنهادی تاریخچه دسترسی به وب هر تب را مدیریت می‌کند. این روش hashCode نمای نمایش‌دهنده وب‌سایت را برای شناسایی تب هنگام دسترسی کاربر به یک صفحه وب دریافت می‌کند. مقدار hashCode به طور منحصر به فرد یک نما را شناسایی می‌کند و یک hashCode منحصر به فرد برای هر تب باز شده توسط کاربر ایجاد می‌شود. وقتی کاربر یک تب را باز می‌کند، رویداد `TYPE_VIEW_FOC USED` در نمای با نام کلاس `android.wi dget.FrameLayout` و شناسه منبع null رخ می‌دهد. بنابراین، روش پیشنهادی می‌تواند با مشاهده رویداد `TYPE_VIEW_FOCUSED` از طریق سرویس دسترسی، تشخیص دهد که کاربر یک تب را باز کرده است.

(CM4) استفاده از لینک‌های لنگر را که در همان صفحه وب منتقل می‌شوند، تعیین می‌کند.

روش پیشنهادی آخرین URL دسترسی شده توسط کاربر را با URL دسترسی یافته شده قبل از هر دسترسی به وب مقایسه می‌کند تا مشخص کند که آیا از لینک لنگر استفاده شده است یا خیر. برای مثال، موردی را در نظر بگیرید که در آن کاربر به وب‌سایت‌های مشخص‌شده با URLهای زیر به ترتیب دسترسی پیدا می‌کند:

https://example[.]org/

https://example[.]org/#top

هنگامی که کاربر به وب‌سایتی با URL 2 دسترسی پیدا می‌کند، روش پیشنهادی مقایسه می‌کند که آیا URL 1 با رشته قبل از "#` در URL 2 مطابقت دارد یا خیر. در این مثال، از آنجا که رشته مورد مقایسه همان ``https://example[.] org/` است، روش پیشنهادی می‌تواند تعیین کند که آیا انتقال به دلیل یک لینک لنگر رخ داده است یا خیر.

شکل ۸ فرآیندی را نشان می‌دهد که از طریق آن روش پیشنهادی تغییر مسیر ناشی از یک لینک لنگر را تشخیص می‌دهد. اگر تغییر مسیر در مرحله (۴) توسط یک لینک لنگر ایجاد شود، روش پیشنهادی از تغییر مسیر صرف نظر کرده و زمان سپری شده بین مراحل (۱) و (۵) را محاسبه می‌کند: در این فرآیند، زمان سپری شده ناشی از دسترسی به یک لینک لنگر، زمانی که تغییر مسیرها توسط لینک‌های لنگر به صورت متوالی در یک وب‌سایت بی‌خطر رخ می‌دهند، محاسبه نمی‌شود. بنابراین، هنگام دسترسی به یک سری متوالی از لینک‌های لنگر در یک وب‌سایت بی‌خطر، هیچ گونه مثبت کاذبی شناسایی نمی‌شود.

هنگامی که تغییر مسیرهای متوالی به وب‌سایت‌های مخرب شامل تغییر مسیرها توسط لینک‌های لنگر می‌شوند، روش پیشنهادی می‌تواند آنها را تشخیص دهد زیرا زنجیره‌های آنها به اندازه کافی طولانی هستند.

(CM5) تعیین تغییر مسیرها با کشیدن انگشت

روش پیشنهادی می‌تواند رویداد ``TYPE_VI EW_SCROLLED`` را از طریق سرویس دسترسی مشاهده کند تا عملیات کشیدن انگشت کاربران را تشخیص دهد. هنگامی که دسترسی به وب را بر اساس کشیدن انگشت کاربر تشخیص می‌دهد، آن را تغییر مسیر به یک وب‌سایت مخرب در نظر نمی‌گیرد. همانطور که در شکل ۷ نشان داده شده است، فرآیند تشخیص وب‌سایت‌های مخرب انجام نمی‌شود و اطلاعات این دسترسی وب به سابقه دسترسی اضافه نمی‌شود.

(CM6) تعیین تغییر مسیرها با استفاده از عملیات ورودی کاراکتر.

هنگامی که کاربر متنی را وارد می‌کند، روش پیشنهادی می‌تواند رویداد `CONTENT_CHANGE_TYPE_TEXT` را از طریق سرویس دسترسی مشاهده کرده و عملیات ورودی متن را تشخیص دهد. در چنین مواردی، آن را به عنوان تغییر مسیر به یک وب‌سایت مخرب تشخیص نمی‌دهد و همانطور که در شکل ۷ نشان داده شده است، فرآیند تشخیص وب‌سایت‌های مخرب را انجام نمی‌دهد و اطلاعات این دسترسی وب را به سابقه دسترسی اضافه نمی‌کند.

طراحی و پیاده سازی

متد ``onAccessibilityEvent()`` توسط وقوع تمام رویدادهایی که می‌توانند توسط سرویس دسترسی مشاهده شوند، فراخوانی می‌شود. روش پیشنهادی با استفاده از رویه زیر، اطلاعات مربوط به رویدادهای مشاهده شده را بدست می‌آورد:

۱) نام رویداد با استفاده از متد ``getEventType()`` بازیابی می‌شود.

۲) اگر رویداد بازیابی شده ``TYPE_WINDOW_CONTENT_CHANGED`` یا ``CONTENT_CHANGE_TYPE_TEX`` باشد، متد ``getViewIdResourceName()`` برای بدست آوردن شناسه منبع نمایی که رویداد در آن رخ داده است، استفاده می‌شود.

۳) اگر رویداد در نوار آدرس گوگل کروم رخ داده باشد، متد ``System.currentTimeMillis()`` برای بازیابی مهر زمانی که در آن رخ داده است، استفاده می‌شود. زمان سپری شده با استفاده از این و چندین مهر زمانی قبلی که توسط Threshold_1 تنظیم شده است، همانطور که در بخش IV-E توضیح داده شده است، محاسبه می‌شود.

۴) اگر زمان سپری شده محاسبه شده کوتاه‌تر از Threshold_2 باشد، روش پیشنهادی تعیین می‌کند که یک تغییر مسیر به یک وب‌سایت مخرب رخ داده است.

روش پیشنهادی گوگل کروم را هدف قرار می‌دهد. با این حال، با پشتیبانی از شناسه‌های منبع نوارهای URL سایر مرورگرها، می‌توان از آن برای تشخیص انتقال به وب‌سایت‌های مخرب در سایر مرورگرها نیز استفاده کرد.

ب. ارزیابی برای تنظیم مقادیر آستانه

ارزیابی آستانه

در این ارزیابی، دسترسی به وب با استفاده از مرورگر کروم در اندروید انجام شد و از وب‌سایت‌های سالم و مخرب به عنوان مقاصد دسترسی استفاده شد. مرجع [۱۸]، [۱۹] بر تغییر مسیرها تمرکز کرد و نشان داد که زنجیره‌های تغییر مسیر برای وب‌سایت‌های مخرب طولانی‌تر از وب‌سایت‌های سالم است. با این حال، این مطالعات CMها را برای چنین تغییر مسیرهایی بررسی نکردند. ما «تعداد دفعات تغییر نوار URL» و «زمان سپری شده» در زنجیره تغییر مسیر ایجاد شده هنگام دسترسی به این وب‌سایت‌ها را ارزیابی کردیم. بر اساس نتایج، مقادیر مناسب برای Threshold_1 و Threshold_2 را همانطور که در بخش IV-E توضیح داده شده است، تنظیم کردیم. یک تنظیم مناسب برای Threshold_1 می‌تواند نرخ مثبت کاذب تغییر مسیرها به وب‌سایت‌های بی‌خطر را سرکوب کرده و نرخ تشخیص آن‌ها به وب‌سایت‌های مخرب را بهبود بخشد، در حالی که برای Threshold_2 می‌تواند دقت تشخیص روش پیشنهادی را افزایش دهد. با این حال، اگر مقادیر آن‌ها خیلی بزرگ باشد، روش پیشنهادی احتمالاً انتقال به وب‌سایت‌های بی‌خطر را به اشتباه تشخیص می‌دهد. با این حال، اگر مقادیر آن‌ها بسیار کوچک باشد، روش پیشنهادی احتمالاً انتقال به وب‌سایت‌های مخرب را از دست می‌دهد.

برنامه مورد استفاده در این ارزیابی، نمونه اولیه برنامه حسگر مورد استفاده در آزمایش WarpDrive بود (که در بخش VI-A توضیح داده شده است). این روش پیشنهادی را با استفاده از سرویس دسترسی اندروید پیاده‌سازی می‌کند و اطلاعات (مانند نتایج تشخیص و زمان‌های تغییر نوار URL) را جمع‌آوری می‌کند. برنامه نمونه اولیه نیز همان اطلاعات برنامه حسگر را جمع‌آوری کرد.

ارزیابی مقادیر آستانه

وب‌سایت‌های بی‌خطر مورد استفاده در ارزیابی، آن‌هایی بودند که در رتبه ۱۵۰ در سایت‌های برتر الکسا (ژاپن) [۱۷] از ۷ اکتبر ۲۰۲۰ قرار داشتند.

این آزمایش با هدف ارزیابی اینکه آیا و تا چه حد برای وب‌سایت‌های بی‌خطری که تغییر مسیرهای متوالی ایجاد می‌کنند، مثبت کاذب رخ می‌دهد، با هدف قرار دادن وب‌سایت‌های بی‌خطری که تغییر مسیرهای متوالی ایجاد می‌کنند، انجام شد. محیط ارزیابی برای یک وب‌سایت بی‌خطر در جدول ۱ (الف) ارائه شده است که شامل مراحل زیر است:

انجام عملیاتی (مثلاً ورود، خروج و لمس تبلیغات) که اغلب منجر به تغییر مسیر به وب‌سایت‌های بی‌خطر می‌شود.

عملیات مربوط به استفاده از هر وب‌سایت را انجام دهید (مثلاً مرور صفحات محصول در یک وب‌سایت خرید).

پس از انجام عملیات شرح داده شده در مرحله ۲، عملیات "برگشت" به صورت متوالی انجام می‌شود.

اگر در مرحله ۱ تغییر مسیر رخ دهد، تعداد دفعاتی که نوار URL تغییر مسیر می‌دهد ثبت می‌شود.
زمان سپری شده برای هر مرحله ۱ و ۳ در هر وب‌سایت ثبت می‌شود.
در مرحله بعد، وب‌سایت‌های مخرب مورد استفاده در ارزیابی که تغییر مسیرهای متوالی ایجاد کردند، ۳۳ وب‌سایت فرود بودند که با استفاده از روش به کار رفته در [۲۰] جمع‌آوری شده بودند و تا ۷ ژوئیه ۲۰۲۰ به عنوان تولیدکننده تغییر مسیرهای خودکار شناخته می‌شدند. ارزیابی در سه محیط اندروید ذکر شده در جدول ۱ با استفاده از فرآیند زیر انجام شد:
در صفحه فرود هر وب‌سایت، با ضربه زدن روی هر نقطه از صفحه، یک تغییر مسیر به یک وب‌سایت مخرب ایجاد می‌شود.
تعداد دفعاتی که نوار URL به دلیل تغییر مسیر از وب‌سایت فرود به یک وب‌سایت مخرب تغییر مسیر می‌دهد، ثبت می‌شود. ۳) زمان سپری شده برای تغییر مسیر ثبت می‌شود.

نتایج ارزیابی برای THRESHOLD_1

تعداد و فراوانی تغییرهای متوالی نوار URL به دلیل تغییر مسیرها در وب‌سایت‌های بی‌خطر و مخرب که در بخش قبلی ثبت شده‌اند، در جدول ۲ فهرست شده‌اند. فراوانی نسبی تغییرهای متوالی در نوار URL به دلیل تغییر مسیرها در شکل ۹ نشان داده شده است. نتایج نشان می‌دهد که تعداد دفعاتی که نوار URL به دلیل تغییر مسیرها تغییر می‌کند، برای وب‌سایت‌های بی‌خطر کم و برای وب‌سایت‌های مخرب زیاد است. به طور خاص، اکثر وب‌سایت‌های بی‌خطر یک یا دو تغییر را متحمل می‌شوند، در حالی که اکثر وب‌سایت‌های بدخیم سه یا چند تغییر را متحمل می‌شوند. بنابراین، تنظیم Threshold_1 روی سه می‌تواند نرخ مثبت کاذب را کاهش دهد(تشخیص تغییر مسیر در وب‌سایت‌های بی‌خطر و جلوگیری از گم شدن وب‌سایت‌های مخرب) از این رو، Threshold_1 را روی سه تنظیم می‌کنیم.
شکل ۱۰ نمودارهایی را نشان می‌دهد که زمان‌های سپری‌شده و فراوانی‌های نسبی تجمعی آن‌ها را در محیط‌های موبایل Wi-Fi، IIJ و Y! برای وب‌سایت‌های بی‌خطر ثبت‌شده در آزمایش‌های شرح داده شده در بخش V-B2 نشان می‌دهد. محورهای افقی زمان‌های سپری‌شده و محورهای عمودی فراوانی نسبی تجمعی آن‌ها را نشان می‌دهند. خط آبی نشان‌دهنده نرخ مثبت کاذب در زمانی است که هیچ CM استفاده نشده است، در حالی که خطوط نارنجی، سبز، خاکستری و قرمز نشان‌دهنده نرخ‌های مثبت کاذب در زمانی هستند که شناسایی شیرهای لینک (CM 1)، شناسایی عملیات "بازگشت" (CM 2)، لیست سفید (CM 3) و CMها ۱۳ اعمال می‌شوند. بدیهی است که روش پیشنهادی با اعمال CMها ۱۳، اکثر مثبت‌های کاذب را سرکوب می‌کند و در نتیجه اثربخشی آن‌ها را نشان می‌دهد. علاوه بر این، تغییر Threshold_2 به مقدار کافی طولانی ۶۰۰۰ میلی‌ثانیه، نرخ مثبت کاذب را در همه محیط‌ها به ۲٫۵٪ کاهش می‌دهد.
زمان سپری شده و فراوانی نسبی تجمعی آن برای تغییر مسیرهای متوالی به وب‌سایت‌های مخرب در شکل ۱۱ نشان داده شده است. خطوط آبی، نارنجی و خاکستری به ترتیب نتایج را برای محیط‌های موبایل Wi-Fi، IIJ و Y! نشان می‌دهند.
تنظیم Threshold_2 به مقدار کافی بزرگ ۱۰۰۰۰ میلی‌ثانیه منجر به نرخ تشخیص ۸۴٫۹، ۹۰٫۹ و ۸۴٫۹٪ به ترتیب برای محیط‌های موبایل Wi-Fi، IIJ و Y! شد. با این حال، هنگامی که روی ۶۰۰۰ میلی‌ثانیه تنظیم شد، نرخ تشخیص در هر دو مورد بیشتر از ۷۰٪ بود.
بنابراین، تنظیم Threshold_2 به ۱۰۰۰۰ میلی‌ثانیه، نرخ تشخیص روش پیشنهادی را بهبود بخشید. با این حال، انتظار نمی‌رود برخی از وب‌سایت‌های بی‌خطر توسط CMهای شرح داده شده در بخش IV-F سرکوب شوند. در این مورد، ما انتظار داریم که تنظیم Threshold_2 روی ۱۰۰۰۰ میلی‌ثانیه ممکن است منجر به تشخیص‌های نادرست بسیاری از تغییر مسیرها به وب‌سایت‌های بی‌خطر شود. بنابراین، Threshold_2 روی ۶۰۰۰ میلی‌ثانیه تنظیم شد که انتظار می‌رود نرخ تشخیص بیش از ۷۰٪ را برای تغییر مسیرها به وب‌سایت‌های مخرب فراهم کند.
از آنجا که روش پیشنهادی به عنوان یک برنامه اندروید پیاده‌سازی شده است، نصب آن مشابه هر برنامه اندروید دیگری است. بنابراین، هر کاربر اندروید می‌تواند به راحتی آن را نصب کند. علاوه بر این، رویدادهایی که می‌توانند مشاهده شوند و اطلاعاتی که می‌توانند از طریق سرویس دسترسی بازیابی شوند، به نسخه اندروید بستگی دارند. عملکرد سرویس دسترسی مورد استفاده در روش پیشنهادی روی اندروید نسخه ۴٫۳ و بالاتر کار می‌کند. در سال ۲۰۲۲، ۹۹٫۷۶٪ از کل دستگاه‌های اندروید در سراسر جهان اندروید ۴٫۳ و بالاتر را اجرا می‌کردند [۲۱]. بنابراین، اکثر دستگاه‌های اندروید می‌توانند از روش پیشنهادی استفاده کنند.
ارزیابی
برای ارزیابی روش پیشنهادی بر روی استفاده واقعی کاربر، داده‌ها از پروژه پاسخ حمله مبتنی بر وب با ابتکار تحقیقات کاربردی قابل استقرار (WarpDrive) [9] جمع‌آوری شدند، که یک سیستم مشاهده حمله مبتنی بر وب است که برای درک رفتارهای حملات

مبتنی بر وب استفاده می‌شود. برای مشاهده دسترسی به وب در گوشی‌های هوشمند، یک برنامه حسگر روی گوشی هوشمند شرکت‌کننده نصب می‌شود و تاریخچه دسترسی به وب، تاریخچه نمایش برنامه و داده‌های اطلاعات دستگاه آنها را جمع‌آوری می‌کند. بنابراین، پس از اجرای روش پیشنهادی، از جمله تصمیمات مربوط به تغییر مسیرهای متوالی به وب‌سایت‌های مخرب، محتوای نوار URL و مقدار hashCode تب باز، جمع‌آوری شد.

لاگ‌های فهرست‌شده در جدول ۳ برای ارزیابی روش پیشنهادی بر روی داده‌های تجربی استفاده شدند. برای نشان دادن اثربخشی CMهای به‌کاررفته در روش پیشنهادی، نتایج روش مرسوم که CMهای ۱ و ۳ را پیاده‌سازی می‌کند و روش پیشنهادی که CMهای ۱ و ۶ را پیاده‌سازی می‌کند، مقایسه شدند. در طول ارزیابی، URLهای نشان داده‌شده توسط لاگ تشخیص و URLهای قبل و بعد از دسترسی به آن و نتایج تشخیص ریدایرکت‌های متوالی به وب‌سایت‌های مخرب ارزیابی شدند. این ارزیابی از ۱۱ آوریل ۲۰۲۲ تا ۱۶ ژوئن ۲۰۲۲ انجام شد. محیط‌های ارزیابی و نتایج به ترتیب در جداول ۴ و ۵ ارائه شده‌اند.

تعداد موارد مثبت کاذب برای روش مرسوم هنوز بالا و برابر با ۱۲۹۴ است که با استفاده از روش پیشنهادی با ۱۰۷۶ مورد (٪۸۳,۱) کاهش به ۲۱۸ مورد رسیده است. بنابراین، نرخ مثبت کاذب فوق‌العاده پایین بود: تقریباً ٪۰,۰۵۴ از کل تعداد گزارش‌ها (۴۰۲۳۳۳) که در جدول ۳ فهرست شده‌اند. علاوه بر این، از آنجا که موارد مثبت کاذب به ندرت در طول استفاده عادی رخ می‌دهند، تأثیر آنها بر قابلیت استفاده از روش پیشنهادی اندک است. جدول ۶ تعداد موارد مثبت کاذب کاهش یافته با استفاده از هر CM را فهرست می‌کند، که نشان می‌دهد هر CM به طور مؤثر تعداد موارد مثبت کاذب را کاهش داده است.

نتیجه گیری

این مطالعه، مسئله‌ی رو به افزایش هدایت کاربران اندروید به وب‌سایت‌های مخرب را برجسته کرد و روشی را برای تشخیص تغییر مسیرهای ناخواسته به چنین وب‌سایت‌هایی پیشنهاد داد که بر فاصله‌ی زمانی تغییر نوار آدرس گوگل کروم با استفاده از سرویس دسترسی اندروید تمرکز دارد. روش پیشنهادی، بر اساس فاصله‌ی زمانی بین چندین تغییر صفحه‌ی وب، تعیین می‌کند که آیا تغییر صفحات وب، تغییر مسیرهای متوالی به وب‌سایت‌های مخرب هستند یا خیر. فواصل زمانی تغییر مسیرهای متوالی برای وب‌سایت‌های بی‌خطر و مخرب مورد تجزیه و تحلیل قرار گرفت و تعداد تغییرهای نوار آدرس و زمان سپری شده هنگام تغییر مسیرهای متوالی برای تعیین آستانه‌های مناسب ارزیابی شد. علاوه بر این، عوامل مرتبط با تعداد زیاد تشخیص‌های مثبت کاذب برای وب‌سایت‌های بی‌خطر مورد تجزیه و تحلیل قرار گرفت و بر این اساس، شش CM طراحی شد. به طور خاص، از لیست‌های سفید، لمس لینک‌ها، عملیات «بازگشت»، انتقال لینک‌های لنگر در همان صفحه وب، انتقال با کشیدن انگشت و انتقال با تایپ متن برای تمایز بین تغییر مسیرهای متوالی به وب‌سایت‌های بی‌خطر و مخرب استفاده شد. روش پیشنهادی با استفاده از داده‌های تجربی جمع‌آوری‌شده توسط پروژه WarpDrive [9] ارزیابی شد و نتایج نشان داد که تعداد موارد مثبت کاذب برای وب‌سایت‌های بی‌خطر به طور قابل توجهی کاهش یافته و وب‌سایت‌های مخرب با موفقیت شناسایی شده‌اند. بنابراین، نرخ تشخیص وب‌سایت‌های مخرب در دستگاه‌های اندروید بدون جمع‌آوری اطلاعات آنها از قبل بهبود یافته و نرخ مثبت کاذب سرکوب شده است. عملکرد تشخیص تغییر مسیرهای متوالی به وب‌سایت‌های مخرب در برنامه Tachikoma Mobile [22] پیاده‌سازی شده است.

مراجع

[1] Statista: Percentage of mobile device website traf_cworldwide from 1st quarter 2015 to 4th quarter 2023,available from hhttps://www.statista.com/statistics/277125/share-of-website-traf_c-coming-from-mobile-devices/i (accessed 2024_03_07).

[2] McAfee: The McAfee Consumer Mobile Threat Report, available from hhttps://www.mcafee.com/content/dam/consumer/enus/docs/reports/rp-mobile-threat-report-feb-2022.pdfi (accessed 2023_01_10).

[3] Statcounter: Mobile Operating System Market ShareWorldwide, available from hhttps://gs.statcounter.com/os-market-share/mobile/worldwidei (accessed 2024_03_07).

[4] PIXM: Phishing tactics: how a threat actor stole 1M credentialsin 4 months, available from hhttps://pixmsecurity.com/blog/blog/phishing-tactics-how-a-threat-actor-stole-1m-credentials-in-4-months/i(accessed 2023_01_10).

[5] Lin, Y., Liu, R., Divakaran, D.M., Ng, J.Y., Chan, Q.Z., Lu, Y., Si, Y., Zhang, F. and Dong, J.S.: Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages, Proc. 30th USENIX Security Symposium (USENIX Security 21), pp.3793_3810 (2021).

[6] Kim, T., Park, N., Hong, J. and Kim, S.W.: Phishing URL Detection: A Network-based Approach Robust to Evasion, Proc. 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS' 22), pp.1769_1782 (2022).

[7] Aravindhan, R., Shanmugalakshmi, R., Ramya, K., et al.: Certain Investigation on Web Application Security: Phishing Detection and Phishing Target Discovery, Proc. 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), pp.1_10 (2016).

[8] Z. Li, S. Alrwais, X. Wang, and E. Alowaisheq, ``Hunting the red fox online: Understanding and detection of mass redirect-script injections,'' in 2014 IEEE Symposium on Security and Privacy, 2014, pp. 3_18.

[9] WarpDrive, available from hhttps://warpdrive-project.jp/i (accessed 2024_05_15).

[10] Mukaiyama, K., Fujita, M., Shirai, T., Kobayashi, S., Nishigaki, M.: Slyware Prevention: Threat of Websites Inducing Accidental Taps and Countermeasures, Proc. Advances in Network-Based Information Systems (NBiS 2017), pp.539_552 (2017).

[11] Imamura, Y., Orito, R., Chaikaew, K., et al.: Threat Analysis of Fake Virus Alerts Using WebView Monitor, Proc. 2019 Seventh International Symposium on Computing and Networking (CANDAR), pp.28_36 (2019).

[12] Liu, D. and Lee, J.-H.: CNN Based Malicious Website Detection by Invalidating Multiple Web Spams, IEEE Access, Vol.8, pp.97258_97266 (2020).

[13] Shibahara, T., Yagi, T., Akiyama, M., et al.: POSTER: Detecting Malicious Web Pages based on Structural Similarity of Redirection Chains, Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15), pp.1671_1673 (2015).

[14] Stringhini, G., Kruegel, C. and Vigna, G.: Shady Paths: Leveraging Sur_ng Crowds to Detect Malicious Web Pages, Proc. 2013 ACM SIGSAC Conference on Computer; Communications Security (CCS'13), pp.133_144 (2013).

[15] Android Developers: VpnService, available from hhttps://developer.android.com/reference/android/net/VpnServicei (accessed 2023_01_10).

[16] Android Developers: AccessibilityService, available from hhttps://developer.android.com/reference/android/accessibilityservice/AccessibilityServicei (accessed 2022_08_08).

[17] Alexa : Top Sites in Japan, available from hhttps://www.alexa.com/topsites/countries/JPi (accessed 2021_01_22).

[18] Chen, G., Meng, W., Copeland, J.: Revisiting Mobile Advertising Threats with MAdLife, Proceedings of the 2019 World Wide Web Conference (WWW'19), pp.207_217, (2019).

[19] Rastogi, V., Shao, R., Chen, Y., Pan, X., Zou, S., Riley, R.: Are these Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces, Proceedings of Network and Distributed System Security Symposium (NDSS 2016), pp.1_15, (2016).

[20] Ishihara, T., Sato, M., Yamauchi, T.: Method of Generating a Blacklist for Mobile Devices by Searching Malicious Websites, Proceedings of 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), (2020).

[21] StatCounter: Mobile & Tablet Android Version Market Share World-wide, available from hhttps://gs.statcounter.com/os-version-market-share/android/mobile-tablet/worldwidei (accessed 2024_08_15).

[22] Google Play: WarpDrive project, available from hhttps://play.google.com/store/apps/details?id=jp.kddilabs.warpdrive&hl=en_USi (accessed 2024_05_17).