Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Securing the Web: A Study on Look-Alike Domain Detection Using Open-Source Intelligence Tools

Ruchi Sharma[1,*], Bhag Dei Thakur[1], Neelam Kaushik[2], Purnima Chauhan[3]

[1]Department of Forensic Science, Himachal Pradesh University, Summer Hill, Shimla, Himachal Pradesh, India.
[2]Department of Biotechnology, Himachal Pradesh University, Summer Hill, Shimla, Himachal Pradesh, India.
[3]Regional Forensic Science Laboratory, Dharamshala, Himachal Pradesh, India.

Received 03 Jan. 2024; Accepted 29 Apr. 2024; Available Online 02 Jun. 2024

Abstract

In an era characterized by the ubiquity of the internet, the proliferation of online services, and the increasing frequency of cyber threats, the detection of look-alike domains has become a critical component of cybersecurity. The current paper presents an approach for the detection of look-alike domains, leveraging the power of open-source intelligence (OSINT) tools. It included gathering and analyzing a wide range of publicly available data sources, including permutations, WHOIS records, IP information, website content, Geo IP, similarity percentage, name server, and mail server records, and building a comprehensive profile of domains under investigation. Through the application of online search engines, patterns and features that distinguish legitimate domains from their deceptive counterparts were established. The analysis demonstrated that OSINT tools provided significant information about the sample domains and successfully detected 1598 registered look-alike domains among 10 sample domains using dnstwist, while OpenSquat identified 103 squatting domains, 960 active phishing websites, and 53 domains with suspicious certificates across five sample websites. The research contributes to the enhancement of cybersecurity practices by providing a cost-effective and scalable solution for identifying look-alike domains, which can serve as precursors to various online threats, including phishing attacks, malware distribution, and fraud.

I. Introduction

A new era of comfort, connectivity, and commerce has started and has been characterized by the rapidly evolving digital landscape. The breadth of the internet is used by malevolent actors to deceive, defraud, and jeopardize the security and privacy of individuals and organizations. This period is, however, also characterized by an escalating threat landscape [1]. The development of look-alike domains, which are online organizations that imitate legitimate websites with the intention of committing different cybercrimes, such as phishing attacks, malware distribution, and fraud, has become a popular misleading strategy in recent years [2].

A look-alike domain is one that closely resembles a target domain without taking the content of the website into account. It is possible that a domain was exploited in bad faith to obtain financial advan-

Keywords: Cybersecurity, Look-alike domains, Open-source intelligence, Domain analysis, Phishing detection, Malware prevention.

Production and hosting by NAUSS

* Corresponding Author: Ruchi Sharma
Email: drruchisharma14@gmail.com

doi: 10.26735/UGSQ6620

tage from the reputation of the target domain [3]. The process of creating a domain name that can be mistaken for a target domain is known as cybersquatting [4]. Cybersquatters or those who engage in cybersquatting create webpages on squatted domains to deceive users into believing that they are interacting with a legitimate website when they are actually interacting with a counterfeit one [5]. By selling advertisements, counterfeit products, or stealing credentials, cyber squatters attempt to capitalize on brand owners' popularity and reputation [6]. Detecting these lookalike domains presents a formidable challenge owing to their remarkable resemblance to legitimate domains. Furthermore, the vast number of registered lookalike domains daily exacerbates the difficulty in monitoring potentially malicious domains effectively. The dynamic nature of cyber threats and the constant evolution of tactics employed by malicious actors further complicate the task of distinguishing between legitimate and fraudulent domains in real time.

According to a study conducted by Fouchereau and Rychkov (2019), 82% of the surveyed companies reported that they have been subjected to at least one attack related to their domain name system (DNS). On average, these companies experienced 9.45 such attacks, resulting in an estimated average cost of damages amounting to $1,000,000 [7]. In line with this, Fortra's 2023 Domain Impersonation Report highlights that brands encountered an average of 39.4 lookalike domains targeting them each month during the first half of 2023, with a noticeable upward trend. Between January and May, the monthly averages ranged from 27.29 to 37.23 lookalike domains, but a significant surge of over 120% was observed from May to June [8]. Therefore, investing in robust detection mechanisms and staying vigilant against the proliferation of lookalike domains are essential for safeguarding the integrity and security of businesses in today's digital landscape.

The current study embarks on a comprehensive journey to tackle the pervasive issue of look-alike domains by merging the power of open-source intelligence (OSINT) tools, domain analysis, and state-of-the-art cybersecurity resources. These tools are employed to quantify the degree of resemblance between original domains and their look-alike counterparts, shedding light on the extent of deception [9]. The study focuses on the critical task of ferreting out malicious intent. By utilizing the capabilities of VirusTotal [10], urlscan.io [11], and Alienvault [12], in-depth analyses are conducted to identify and classify any registered lookalike domains that pose a threat to cybersecurity.

The main purpose of study is to form a robust framework for identifying, analyzing, and mitigating the risks associated with look-alike domains. By harnessing the potential of OSINT tools, manual comparison techniques, and the collective intelligence of the cyber security community, this research endeavors to fortify the digital realm against deceptive threats, ultimately contributing to the safeguarding of the online world.

II. Materials and Methods

For the data collection and analysis in this investigation, a dedicated computer system was used, featuring two distinct operating environments. First, Windows 10 Pro served as the host operating system for collecting sample domains. Following this, a guest operating system, Kali Linux, was set up within a hypervisor environment using Oracle Virtual Box 6.0.10. This virtualized configuration offered the required flexibility and security measures, facilitating comprehensive analysis of the collected domains. The two operating systems were instrumental in executing a range of detection and analysis activities throughout the investigation.

In order to facilitate the investigation, a total of 10 websites were thoughtfully selected as sample subjects for analysis, encompassing two distinct categories. Among these websites, two were official government websites, chosen due to their critical importance and high trustworthiness. Additionally, eight websites were drawn from the Alexa Top Websites database, a reputable source for ranking websites based on their popularity and traffic. These selections aimed to provide a well-rounded perspective for the study, with the government websites serving as representative examples of trusted sources and the Alexa Top websites offering a cross-section of the most frequently visited sites on the internet, ensuring a comprehensive and diverse sample for analysis. Table I provides a comprehensive listing of each sample website.

Three online scanning engines were employed to evaluate the legitimacy and security of the identified domains. First, VirusTotal was used for in-depth scans of these domains to identify any potential malicious activities, associated files, or links. Second, urlscan.io was utilized to capture and analyze web pages linked to these domains, enabling the detection of potential threats or anomalies. Finally, Alienvault was leveraged to gather additional threat intelligence and cross-reference the identified domains with known malicious entities, enhancing the overall assessment of their security and legitimacy.

III. Results

A. Detection by using Dnstwist

The registered look-alike domains of the original sample websites were obtained by using dnstwist. The significant variation is shown in Table II.

Different types of permutations of registered look-alike domains were found which were used to create the look-alike domain. These permutations are mentioned in Table III.

TABLE I
Sample Websites

Sample websites	Alexa Top website Rank	Website type
www.google.com	1	Multi-tech company website
www.facebook.com	5	Social media website
www.amazon.com	10	e-commerce website
www.instagram.com	11	Social media website
www.microsoft.com	24	Multi-tech company website
www.paypal.com	44	Banking website
www.netflix.com	54	OTT streaming website
www.sbi.co.in	8855	Banking website
www.pmindia.gov.in	-	Government website
www.cbi.gov.in	-	Government website

1) Analysis of reachable look-alike domains by using Virus Total and urlscan.io

Among the 22 look-alike domains with SPYING-MX associated with Google, 10 were reachable and similarly, for SBI, 10 out of the 44 SPYING-MX websites were accessible as illustrated in Fig. 1.

The scanning of all accessible look-alike domains associated with Google (an international domain) and SBI (a national domain) indicated that the malicious squatting domains redirected users to illicit websites, whereas the benign ones tended to guide users back to the original domain names in both domains. The degree of maliciousness associated with a look-alike domain was gauged based on the number of vendors that flagged it. A high number of security vendors indicated that they were more vulnerable to malicious attacks. Furthermore, the analysis extended to urlscan.io, which conducted scans on these look-alike domains. It provided valuable insights such as the domains' associated IP addresses, geographical location of domain operation, registrar information, registrant details, and the date of domain creation. The VirusTotal and UrlScan.io reports of suspicious look-alike domains from Google and SBI are shown in Table IV and V.

TABLE II
Registered Look-Alike Domains of Sample Websites

Sample websites	Total look-alike domains	Registered look-alike domains
www.google.com	3614	221
www.facebook.com	4291	249
www.instagram.com	6640	275
www.amazon.com	3270	217
www.microsoft.com	5500	242
www.paypal.com	1949	151
www.netfkix.com	1855	183
www.sbi.co.in	666	52
www.pmindia.gov.in	4603	3
www.cbi.gov.in	518	5

TABLE III
Types of Permutations

Sample Websites Permutations	www.google. com	www.facebook.com	www.instagram.com	www.amazon.com	www.paypal.com	wwwnetflix.com	www. Microsoft.com	www.sbi.co.in	www.pmindia.gov.in	www.cbi.gov.in
Addition	25	30	29	36	17	30	27	12	-	1
Bitsquatting	9	32	35	22	23	31	28	11	-	1
Homoglyph	98	67	82	49	16	19	40	6	1	1
Cyrillic	1	-	-	-	1	-	-	-	-	-
Hyphenation	4	6	2	5	5	1	4	4	-	-
Insertion	30	53	55	52	41	50	71	1	1	-
Omission	5	7	9	6	5	7	9	2	-	-
Repetition	2	6	7	2	3	3	7	2	-	-
Replacement	29	28	38	28	24	29	33	12	-	1
Subdomain	2	2	2	3	3	2	5	-	-	-
Transposition	4	5	7	5	5	5	8	2	-	-
Various	3	3	3	2	3	3	3	1	1	1
Vowel-swap	7	9	5	6	4	3	6	1	-	-

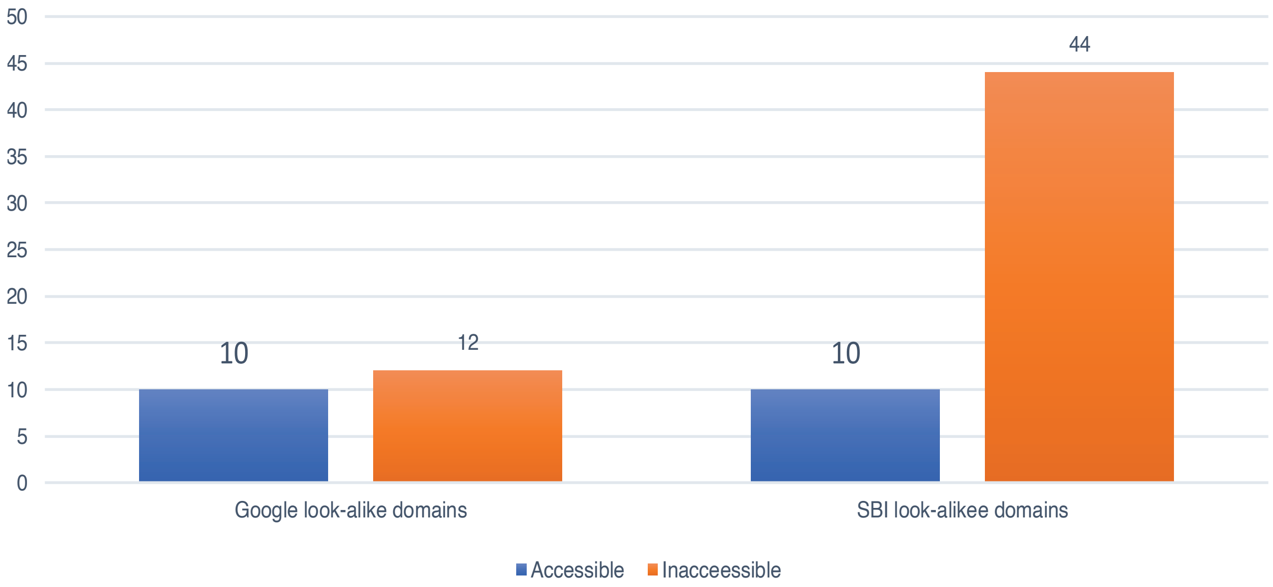
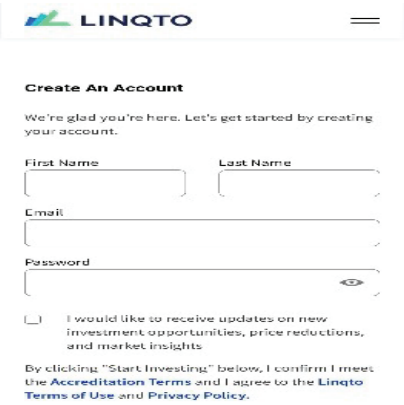
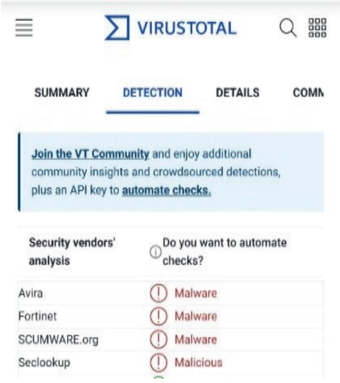
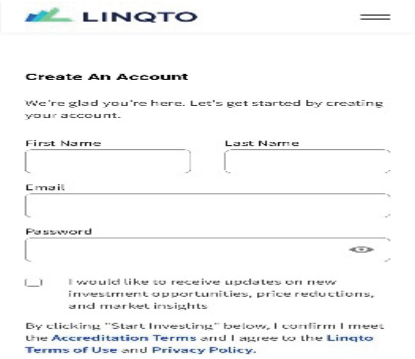
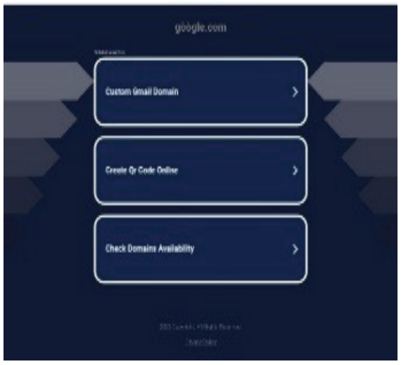
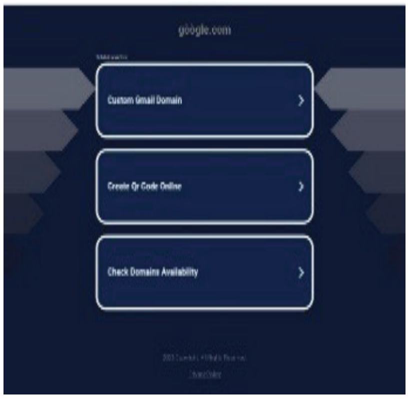
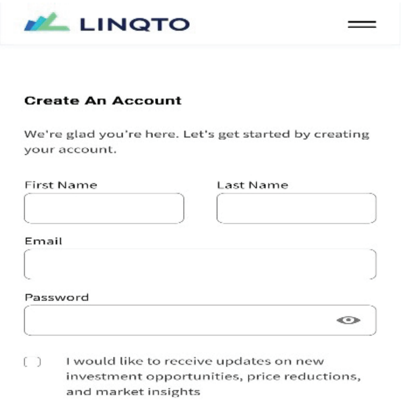
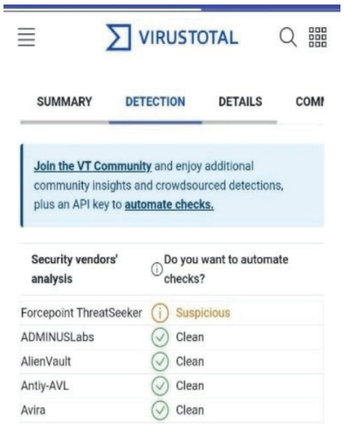
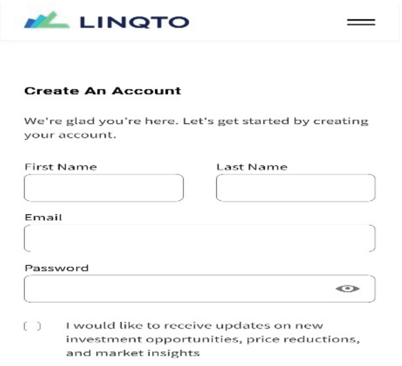
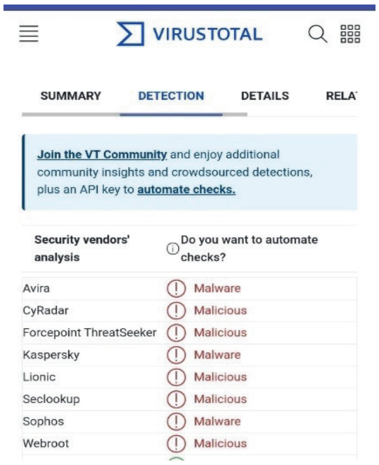
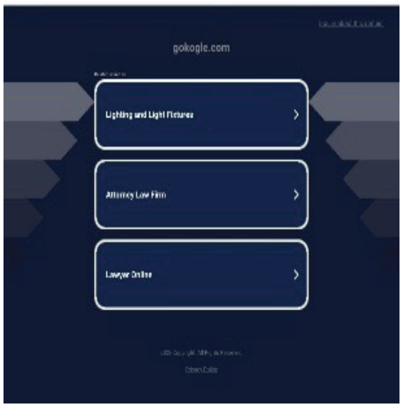
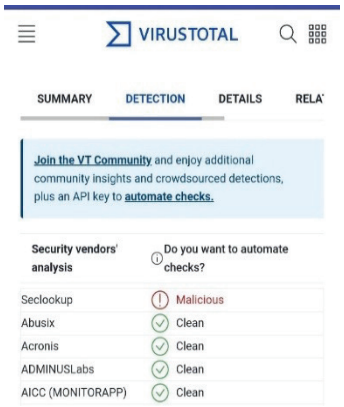
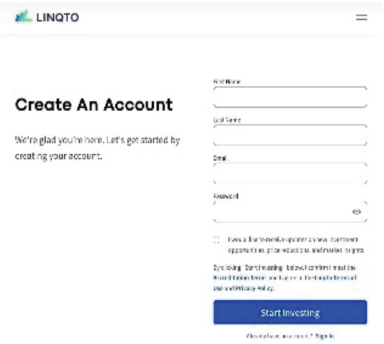
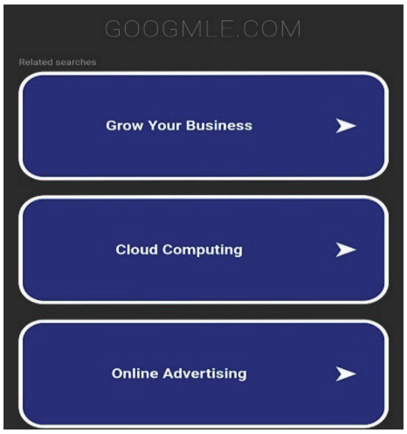
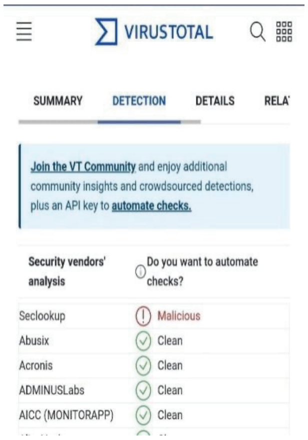


Fig. 1. Number of look-alike domains with SPYING-MX.

TABLE IV
Suspicious look-alike Domains of Google

Sr. no.	Suspicious look-alike domain	Virus total Report	Urlscan.io Report
1.	www.google4.com (Redirects to https://app.linqto.com)  LINQTO Create An Account We're glad you're here. Let's get started by creating your account. First Name Last Name Email Password ☐ I would like to receive updates on new investment opportunities, price reductions, and market insights By clicking "Start Investing" below, I confirm I meet the Accreditation Terms and I agree to the Linqto Terms of Use and Privacy Policy.	4 security vendors out of 80 flagged this domain as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS COMM Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis Do you want to automate checks? Avira Malware Fortinet Malware SCUMWARE.org Malware Seclookup Malicious	Connected IPs: 2 Main IP: 185.53.177.54 Connected domains: 2 Connected countries: 2 Location: Germany Registrant: TEAMINTER-NET-AS, DE Registrar: RIPENCC
2.	www.googleq.com (Redirects to https://app.linqto.com)  LINQTO Create An Account We're glad you're here. Let's get started by creating your account. First Name Last Name Email Password ☐ I would like to receive updates on new investment opportunities, price reductions, and market insights By clicking "Start Investing" below, I confirm I meet the Accreditation Terms and I agree to the Linqto Terms of Use and Privacy Policy.	No security vendors flagged this domain as malicious	Connected IPs: 2 Main IP: 185.53.178.53 Connected domains: 2 Connected countries: 1 HTTP Transactions: 3 Location: Germany Registrant: TEAMINTER-NET-AS, DE Registrar: SAV.COM, LLC Created on: 1 September, 2020.
3.	www.gòògle.com (Alert: Fake website, Redirects to htttp://www.xn—ggle-lqaa.com/)  gòògle.com Custom Gmail Domain Create Qr Code Online Check Domains Availability	No security vendors flagged this domain as malicious	Connected IPs: 5 Main IP: 185.53.177.50 Connected domains: 5 Connected countries: 2 HTTP Transactions: 13 Location: Germany Registrant: TEAMINTER-NET-AS, DE Registrar: GoDaddy.com, LLC Created on: 10 January, 2021.

Sr. no.	Suspicious look-alike domain	Virus total Report	Urlscan.io Report
4.	www.googlė.com (Alert: fake website, Redirects to http://www.xn--googl-b0a.com/)  göögle.com Custom Gmail Domain › Create Qr Code Online › Check Domains Availability ›	No security vendors flagged this URL as malicious	Connected IPs: 5 Main IP: 185.53.178.53 Connected domains: 5 Connected countries: 2 HTTP Transactions: 12 Location: Germany Registrant: TEAMINTER-NET-AS, DE Registrar: NameBright.com DBA TurnCommerce, Inc. Created on: 5 November, 2015 Updated on: 8 January, 2023.
5.	www.goobgle.com (Redirects to https://app.linqto.com/signup?  LINQTO Create An Account We're glad you're here. Let's get started by creating your account. First Name Last Name Email Password ( ) I would like to receive updates on new investment opportunities, price reductions, and market insights	No security vendors flagged this URL as malicious, 1 vendor flagged it as suspicious  VIRUSTOTAL SUMMARY DETECTION DETAILS COMI Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Forcepoint ThreatSeeker ⓘ Suspicious ADMINUSLabs ✓ Clean AlienVault ✓ Clean Antiy-AVL ✓ Clean Avira ✓ Clean	Connected IPs: 7 Main IP: 76.223.26.96 Connected domains: 6 Connected countries: 4 Location: United States Registrant: Amazon-02, US
6.	www.googfle.com Redirects to https://app.linqto.com/signup?  LINQTO Create An Account We're glad you're here. Let's get started by creating your account. First Name Last Name Email Password ( ) I would like to receive updates on new investment opportunities, price reductions, and market insights	8 security vendors out of 88 flagged this domain as malicious  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Avira ⓘ Malware CyRadar ⓘ Malicious Forcepoint ThreatSeeker ⓘ Malicious Kaspersky ⓘ Malware Lionic ⓘ Malicious Seclookup ⓘ Malicious Sophos ⓘ Malware Webroot ⓘ Malicious	Connected IPs: 5 Main IP: 185.53.177.53 Connected domains: 4 Connected countries: 2 Location: Germany Registrant: TEAMINTER-NET-AS Registrar: GoDaddy.com, LLC Created on: 13 November 2008 Updated on: August 8, 2023

Sr. no.	Suspicious look-alike domain	Virus total Report	Urlscan.io Report
7.	www.gokogle.com Redirects to http://www.gokogle.com/)  gokogle.com Lighting and Light Fixtures Attorney Law Firm Lawyer Online	1 security vendor flagged this domain as malicious  Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Seclookup ⓘ Malicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AICC (MONITORAPP) ✓ Clean	Connected IPs: 5 Main IP: 185.53.177.53 Connected domains: 4 Connected countries: 4 HTTP Transactions: 17 Location: Germany Registrant: TEAMINTER-NET-AS Registrar: GoDaddy.com, LLC Created on: 13 November, 2008.
8.	www.goofgle.com Redirects to https://app.linqto.com/signup?)  LINQTO First Name Last Name Email Password Start Investing Sign In Create An Account We're glad you're here. Let's get started by creating your account.	No security vendors flagged this domain as malicious	Connected IPs: 5 Main IP: 185.53.178.50 Connected domains: 4 Connected countries: 2 Location: Germany Registrant: TEAMINTER-NET-AS, DE Registrar: RIPENCC.
9.	www.googmle.com (Redirects to http://ww7.googmle.com/)  GOOGMLE.COM Related searches Grow Your Business Cloud Computing Online Advertising	1 security vendor flagged this domain as malicious  Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Seclookup ⓘ Malicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AICC (MONITORAPP) ✓ Clean	Connected IPs: 4 Main IP: 199.59.243.224 Connected domains: 4 Connected countries: 2 HTTP transactions: 14 Location: United States Registrant: Amazon-02,US Registrar: GoDaddy.com, LLC Created on: 22 February, 2004

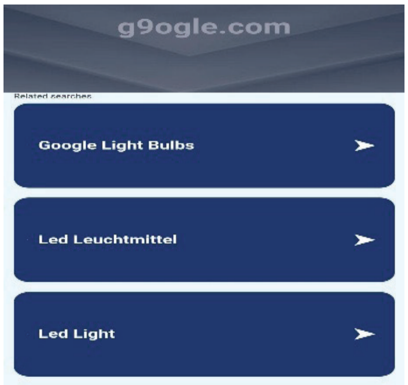
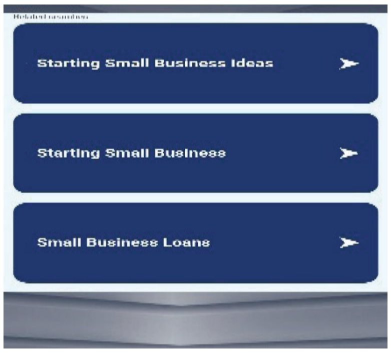
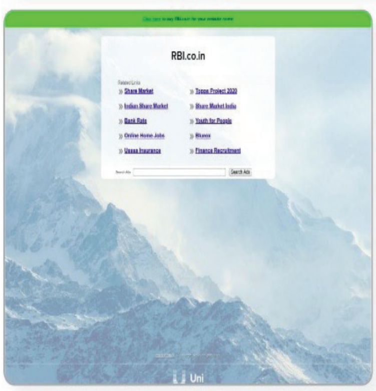
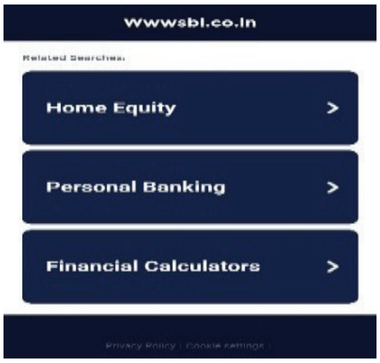
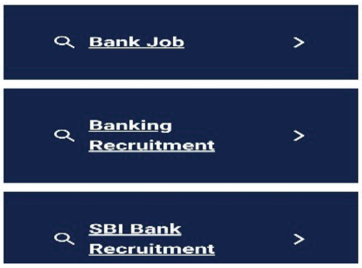
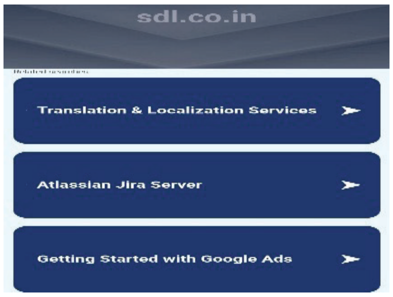
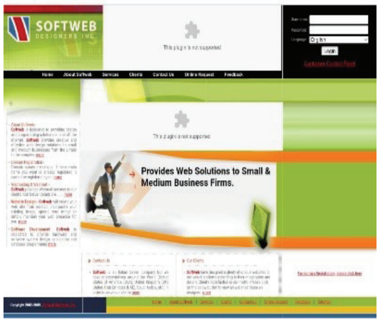
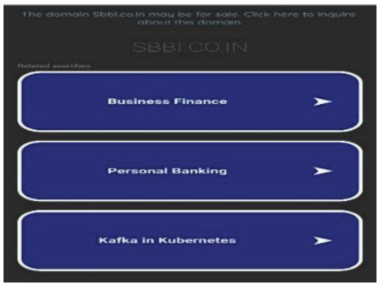
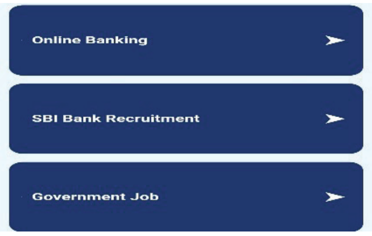
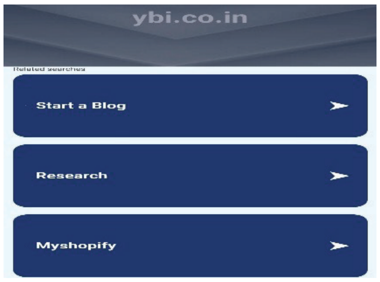
Sr. no.	Suspicious look-alike domain	Virus total Report	Urlscan.io Report
10.	www.g9ogle.com Redirects to http://ww38.g9ogle.com/)  g9ogle.com Related searches Google Light Bulbs Led Leuchtmittel Led Light	No security vendors flagged this domain as malicious	Connected IPs:1 Main IP: 103.224.182.238 Connected domains: 1 Connected countries: 1 HTTP Transactions: 1 Location: Australia Registrant: TRELLIAN-AS-AP Trellian Pty. Limited, AU

TABLE V
Suspicious look-alike Domains of SBI

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
1.	www.sba.co.in (Redirects to http://ww38.sba.co.in/)  Related searches Starting Small Business Ideas Starting Small Business Small Business Loans	No security vendors flagged this URL as malicious	Connected IPs: 7 Main IP: 92.223.51.163 Connected domains: 12 Main domain: join.worldoftanks.asia Connected countries: 2 HTTP Transactions: 33 Registrar: Dynadot LLC Created: August 25th, 2011 Updated: July 31st, 2023 Expiry: August 25th, 2024
2.	www.rbi.co.in (Redirects to http://www.rbi.co.in/)  Click here to buy RBI.co.in for your website name RBI.co.in Related Links Share Market Topps Project 2020 Indian Share Market Share Market India Bank Rate Youth for People Online Home Jobs Bitcoin Ujjain Insurance Finance Recruitment Search Ads Search Ads Uni	No security vendors flagged this URL as malicious	Connected IPs: 5 Main IP: 185.53.178.53 Connected domains: 5 Connected countries: 2 Location: Germany Registrant: TEAMINTERNET-AS, DE Registrar: Name.com, Inc. Created on: June 28th, 2006 Updated on: June 17th, 2023 Expiry: June 28th, 2024

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
3.	wwwsbi.co.in (Redirects to http://wwwsbi.co.in/)  Wwwsbi.co.in Related Searches: Home Equity > Personal Banking > Financial Calculators > Privacy Policy | Cookie settings	No security vendors flagged this URL as malicious	Connected IPs: 2 Main IP: 185.53.177.50 Connected domains: 2 Connected countries: 2 HTTP Transactions: 2 Location: Germany Registrant: TEAMINTERNET-AS, DE Registrar: Dynadot LLC Created on: May 15th, 2023 Updated on: August 22nd, 2023 Expiry: May 15th, 2024
4.	www.sbl.co.in (Redirects to http://ww38.sbl.co.in/)  Bank Job > Banking Recruitment > SBI Bank Recruitment >	No security vendors flagged this URL as malicious	Connected IPs: 7 Main IP: 92.223.51.163 Connected domains: 12 Main domain: join.worldoftanks.asia Connected countries: 3 Registrar: Dynadot LLC Created on: May 20th, 2011 Updated on: February 21st, 2023 Expiry: May 20th, 2024
5.	www.sdl.co.in (Redirects to http://www.sdl.co.in/)  sdl.co.in Related searches: Translation & Localization Services Atlassian Jira Server Getting Started with Google Ads	No security vendors flagged this URL as malicious	Connected IPs: 5 Main IP: 185.53.178.14 Connected domains: 5 Main domain: www.sdl.co.in Connected countries: 2 HTTP Transactions: 13 Location: Germany Registrant: TEAMINTERNET-AS, DE Registrar: GoDaddy.com, LLC Created on: June 3rd, 2009 Updated on: May 14th, 2023 Expiry: June 3rd, 2024
6.	www.sdi.co.in (Redirects to https://www.sdi.co.in/)p  SOFTWEB DESIGNERS INC This plugin is not supported Login Customer Control Panel Home About SofTweb Services Clients Contact Us Online Request Feedback This plugin is not supported Provides Web Solutions to Small & Medium Business Firms. Contact Us Our Clients	No security vendors flagged this URL as malicious	Connected IPs: 5 Main IP: 50.28.37.90 Connected domains:1 Connected countries:1 HTTP transactions: 49 Location: United States Registrant: LIQUIDWEB, US Registrar: Endurance Digital Domain Technology LLP Created on: August 21st, 2005 Updated on: August 19th, 2023 Expiry: August 21st, 2024

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
7.	www.sbbi.co.in Redirects to http://ww25.sbbi.co.in/)  The domain Sbbi.co.in may be for sale. Click here to inquire about this domain. SBBI.CO.IN Related searches Business Finance Personal Banking Kafka in Kubernetes	No security vendors flagged this URL as malicious	Connected IPs: 7 Main IP: 199.59.243.224 Connected domains: 6 Connected countries: 2 HTTP Transactions: 16 Location: United States Registrant: AMAZON-02, US Registrar: TLD Registrar Solutions Ltd. Created on: May 13th, 2022 Updated on: May 16th, 2023 Expiry: May 13th, 2024
8.	www.sni.co.in (Redirects to http://ww38.sni.co.in/)  	No security vendors flagged this URL as malicious	Connected IPs: 7 Main IP: 92.223.51.163 Connected domains: 12 Main domain: join.worldoftanks.asia Connected countries: 1 HTTP transactions: 33 Registrar: Dynadot LLC Created on: January 31st, 2012 Updated on: February 6th, 2023 Expiry: January 31st, 2024
9.	www.ybi.co.in (Redirects to http://www.ybi.co.in/)  ybi.co.in Related searches Start a Blog Research Myshopify	No security vendors flagged this URL as malicious	Connected IPs: 5 Main IP: 185.5.177.54 Connected domains: 5 Connected countries: 2 Location: Germany Registrant: TEAMINTERNET-AS, DE Registrar: GoDaddy.com, LLC Created on: 26 June, 2019 Updated on: 12 June, 2023 Expiry: 26 June, 2024.
10.	www.sbe.co.in (Redirects to http://www.sbe.co.in/)	No security vendors flagged this domain as malicious	Connected IPs: 5 Main IP: 185.53.177.52 Connected domains: 5 Connected countries: 2 Location: Germany Registrant: TEAMINTERNET-AS, DE Registrar: Dynadot LLC Created on: 20 April, 2022 Updated on: 21 February, 2023 Expiry: 20 April, 2024.

2) Detection of Webpage Similarity Degree

Out of the 10 sample domains, 7 had look-alike domains that exhibited webpage similarity to the original domain. The recorded webpage similarity data is presented in Table VI and VII. Interestingly, there were no look-alike domains found for Instagram, SBI, and PM India that showed any webpage similarity. However, in the case of Amazon, out of the 270 registered look-alike domains, a substantial 135 of them displayed a very high webpage similarity percentage, ranging from 65% to 99% as illustrated in Fig. 2. Notably, each of these look-alike domains, with webpage similarity percentages spanning from 30% to 98%, consistently redirected users to the original domain itself.

3) Analysis of suspicious mail servers using AlienVault

Six common mail servers from all look-alike domains of sample websites, using dnstwist, were identified as suspicious since they were marked as 'SPYING-MX.' The suspicious mail servers were park-mx.above.com, mail.h-email.net, mail.hope-mail.com, mx156.hostedmxserver.com, mail.mailerhost.net, and mail.nickstel.com. AleinVault's analysis report provided a comprehensive overview, including the verdict on their suspicious nature, the IP addresses associated with them, their geographical locations, the name servers they utilized, relevant tags, and notably, the number of malicious files communicating with these servers. Additionally, the analysis disclosed the types of malwares detected by antivirus software and their corresponding detection ratios.

TABLE VI
Webpage Similarity Percentage

Sr. No.	Look-alike Domains of Google	Webpage similarity percentage (TLSH)	Look-alike Domains of Facebook	Webpage similarity percentage (TLSH)	Look-alike Domains of Paypal	Webpage similarity percentage (TLSH)
1.	www.google.com	15%	www.facebookx.com	8%	www.paypa-l.com	10%
2.	www.googlē.com	97%	www.fąçebook.com	11%	www.paypla.com	13%
3.	www.googic.com	15%	www.faceboôk.com	11%	-	-
4.	www.ĝoogle.com	34%	www.faceb9ook.com	21%	-	-
5.	www.g-oogle.com	4%	www.faceboiok.com	20%	-	-
6.	www.gpoogle.com	96%	-	-	-	-
7.	www.googl.com	96%	-	-	-	-
8.	www.gogle.com	96%	-	-	-	-
9.	www.gooogle.com	97%	-	-	-	-
10.	www.googlr.com	97%	-	-	-	-
11.	www.googel.com	95%	-	-	-	-
12.	www.goolge.com	97%	-	-	-	-
13.	www.gogole.com	96%	-	-	-	-
14.	wwwgoogle.com	96%	-	-	-	-

TABLE VII
WEBPAGE SIMILARITY PERCENTAGE

Sr. No.	Look-alike Domains of Microsoft	Webpage similarity percentage (TLSH)	Look-alike Domains of Netflix	Webpage similarity percentage (TLSH)	Look-alike Domains of CBI	Webpage similarity percentage (TLSH)
1.	www.microsoft9.com	33%	www.nētflix.com	18%	www.cci.gov.in	20%
2.	www.micro3oft.com	18%	www.netfplix.com	25%	www.cbi.in	6%
3.	www.macrosoft.com	48%	-	-	-	-
4.	www.micropsoft.com	55%	-	-	-	-
5.	www.microsort.com	34%	-	-	-	-
6.	www.microxoft.com	14%	-	-	-	-

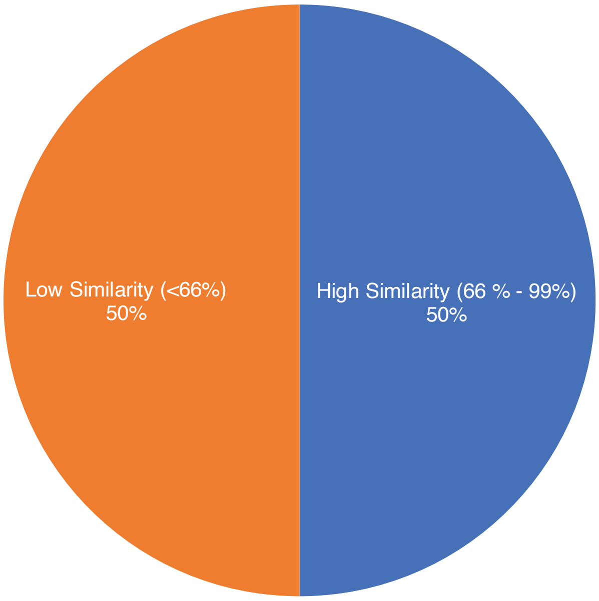


Fig. 2. Number of registered look-alike domains of Amazon.

B. Detection by Using OpenSquat

A total of 155,298 domains from 5 sample websites were detected by OpenSquat. The findings revealed the presence of 103 registered look-alike domains employed in domain squatting, 960 active phishing websites, 53 domains with suspicious certificates, and 6 websites with webpage similarity confidence levels as presented in Fig. 3.

1) Checking for Reachable Websites

The domain-squatted websites, domains with suspicious certificates, and the active phishing websites of Microsoft, Amazon, and Google, respectively, were checked to see whether they were reachable to the user or not, using the 'ping' command in the command prompt. Of the 11 detected Microsoft websites with squatted domains, 8 were reachable. Regarding domains with suspicious certificates, out of the 14 detected Amazon look-alike domains, 10 were reachable, and 11 out of 25 Google websites were also found to be accessible as active phishing websites as illustrated in Fig. 4.

2) Analysis of Microsoft's domain squatted websites by using VirusTotal and UrlSacn.io

A VirusTotal report showed that 4 websites out of 8 were tagged as malicious and phishing by some vendors. UrlScan.io showed information about the IP address, geolocation, created date, and registrar of the suspicious look-alike domains of Microsoft, as shown in Table VIII.

3) Analysis of Amazon's domains with suspicious certificates by using VirusTotal and UrlSacn.io

Ten suspicious lookalike websites of Amazon with suspicious certificates were analyzed by using VirusTotal and UrlScan.io. 7 websites were flagged as malicious and phishing by using VirusTotal, and numbers of IPs operated by domain, number of transactions, the main IP, created time, and domain registrar information were obtained by using UrlScan.io, as illustrated in Table IX.

4) Analysis of active phishing websites of Google by using VirusTotal and UrlSacn.io

A total of 11 websites, which were accessible and functional, have been scanned and analyzed. Interestingly, all these websites received malicious and phishing designations from various VirusTotal vendors, with one exception: the website account. google.com.notecua.inf.br. For this particular website, UrlScan.io generated a report containing information on the number of IP addresses associated with the domain, transaction counts, the primary IP address, creation timestamp, and domain registrar details. Additionally, four websites received a verdict of "Potentially Malicious" as shown in Table X.

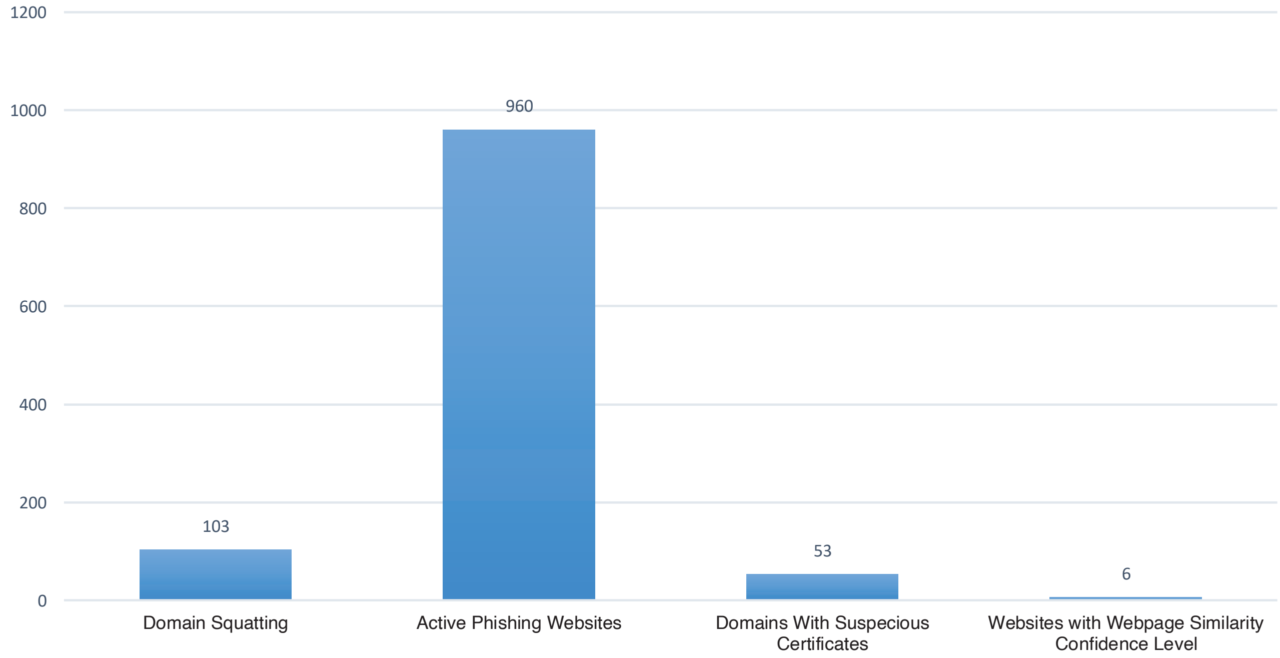


Fig. 3. Number of registered look-alike domain detected by using Open-Squat.

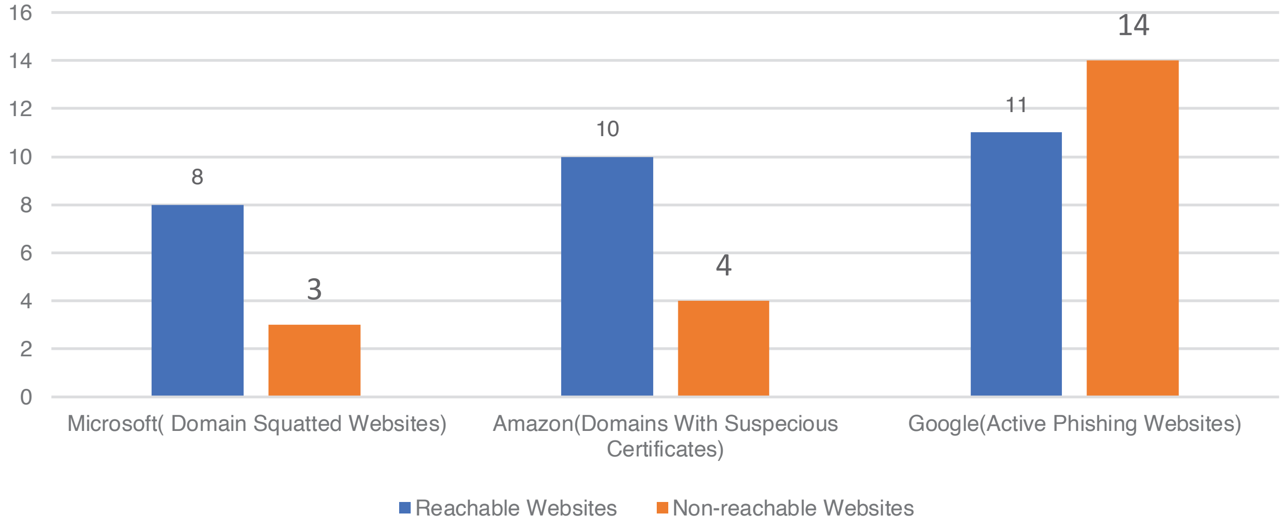
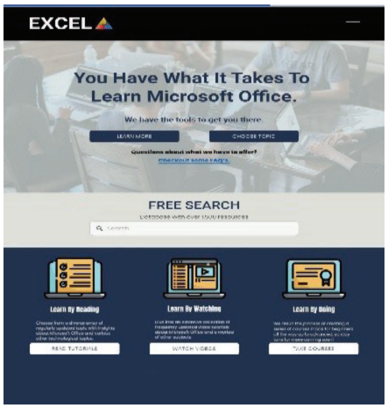
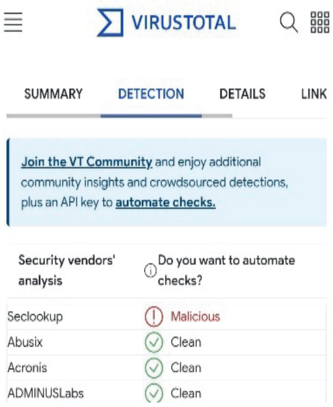
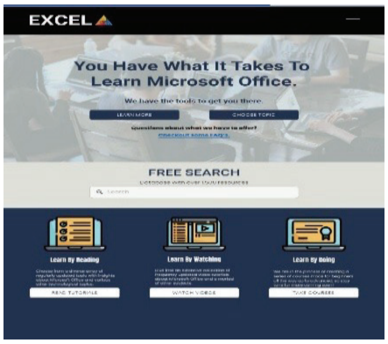
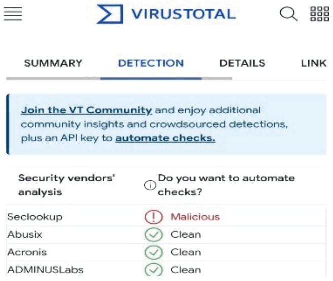
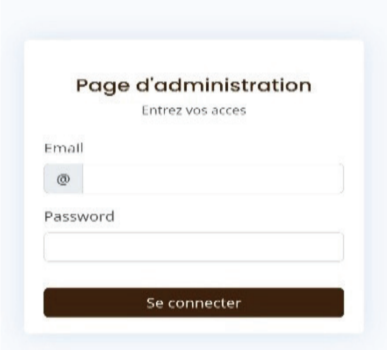
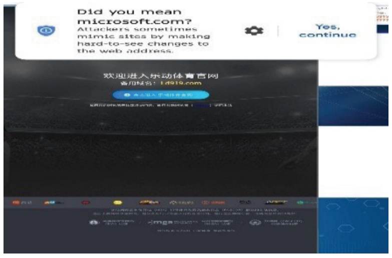
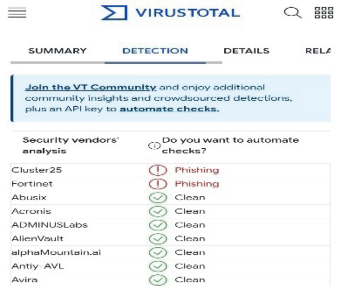
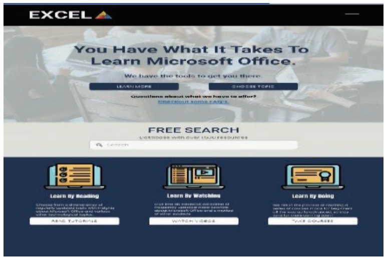
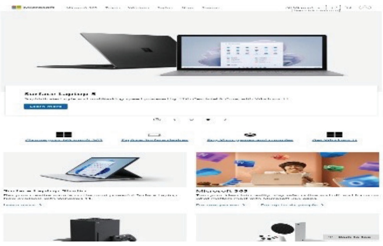
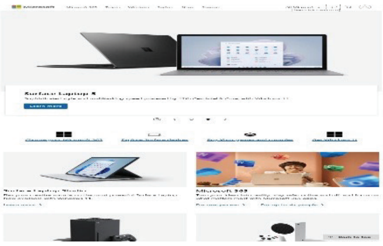


Fig. 4. Number of reachable websites of Microsoft, Amazon and Google.

TABLE VIII
Suspicious look-alike Domains of Microsoft

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
1.	364microsoft.com (Redirects to https://www.exceldelta.com/  EXCEL You Have What It Takes To Learn Microsoft Office. We have the tools to get you there. LEARN MORE CHOOSE TOPIC Questions about what we have to offer? Checkout some FAQ's. FREE SEARCH Search Learn By Reading READ TUTORIALS Learn By Watching WATCH VIDEOS Learn By Doing TAKE COURSES	1 security vendor flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS LINK Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis Do you want to automate checks? Seclookup: Malicious Abusix: Clean Acronis: Clean ADMINUSLabs: Clean	Connected IPs: 15 Main IP: 198.49.23.144 Connected domains: 14 Connected countries: 2 HTTP Transactions: 69 Location: United States Registrant: SQUARESPACE, US Registrar: Squarespace Domains, LLC Created on: July 23rd 2023
2.	366microsoft.com (Redirects to https://www.exceldelta.com/  EXCEL You Have What It Takes To Learn Microsoft Office. We have the tools to get you there. LEARN MORE CHOOSE TOPIC Questions about what we have to offer? Checkout some FAQ's. FREE SEARCH Search Learn By Reading READ TUTORIALS Learn By Watching WATCH VIDEOS Learn By Doing TAKE COURSES	1 security vendor flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS LINK Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis Do you want to automate checks? Seclookup: Malicious Abusix: Clean Acronis: Clean ADMINUSLabs: Clean	Connected IPs: 15 Main IP: 198.185.159.144 Connected domains: 14 Connected countries: 2 HTTP Transaction: 70 Location: United States Registrar: Squarespace Domains, LLC Created on: July 23rd 2023
3.	4microsoft.com Alert- Dangerous website (Redirects to https://4microsoft.com/)  Page d'administration Entrez vos acces Email @ Password Se connecter	No security vendors flagged this URL as malicious	Connected IPs: 3 Main IP: 192.162.71.46 Connected domains: 3 Connected countries: 2 HTTP transaction: 23 Location: France Registrant: LWS, FR TEAM-INTERNET-AS, DE Registrar: GoDaddy.com, LLC Created on: July 22nd, 2023 Updated on: July 22nd, 2023

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
4.	eopen-microsoft.com (Redirects to https://www.eopen-microsoft.com/)  Did you mean microsoft.com? Attackers sometimes mimic sites by making hard-to-see changes to the web address. Yes, continue 欢迎进入乐动体育官网 备用域名：ld919.com	2 security vendors flagged this domain as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis — Do you want to automate checks? Cluster25 — Phishing Fortinet — Phishing Abusix — Clean Acronis — Clean ADMINUSLabs — Clean AlienVault — Clean alphaMountain.ai — Clean Antiy-AVL — Clean Avira — Clean	Connected IPs: 4 Main IP: 154.212.212.149 Connected domains: 4 Connected countries: 2 Location: Hong Kong Registrant: MYCLOUD-AS-AP LUOGELANG FRANCE LIMITED, HK TEAMINTER-NET-AS, DE Registrar: APNIC
5.	Microsoft367.com (Redirects to https://www.exceldelta.com/  EXCEL You Have What It Takes To Learn Microsoft Office. We have the tools to get you there. LEARN MORE CHOOSE TOPIC FREE SEARCH Learn By Reading — READ TUTORIALS Learn By Watching — WATCH VIDEOS Learn By Doing — TAKE COURSES	No security vendors flagged the redirected URL as malicious.	Connected IPs: 15 Main IP: 198.49.23.145 Connected domains: 14 Connected countries: 2 Location: United States Registrant: SQUARESPACE, US Registrar: Squarespace Domains, LLC Created on: 23 July, 2023
6.	Microsoft.sl (Redirects to https://www.microsoft.com/en-in/ 	No security vendors flagged this URL as malicious	Connected IPs: 35 Main IP: 23.223.49.154 Connected domains: 45 Connected countries: 5 HTTP transaction: 147 Location: Sydney, Australia Registrant:VOCUS-RETAIL-AU Vocus Retail, AU TEAMINTERNET-AS, DE Registrar: MarkMonitor, Inc. Created on: May 2nd 1991
7.	Selfmicrosoft.com (Redirects to https://www.microsoft.com/en-in/ 	No security vendors flagged this URL as malicious	Connected IPs: 11 Main IP: 2a02:26f0:3100:1ad::356e Connected domains: 8 Connected countries: 3 HTTP transactions: 85 Location: Frankfurt am main, Germany Registrant: AKAMAI-ASN1, NL Registrar: MarkMonitor, Inc Created on: 2 May, 1991.

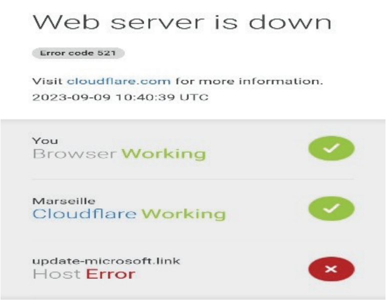
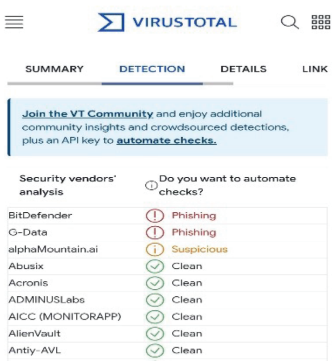
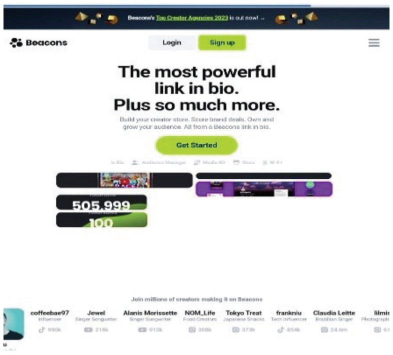
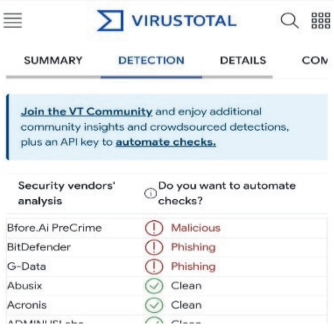
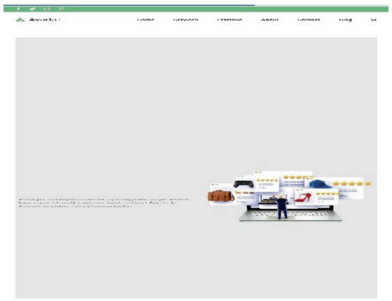
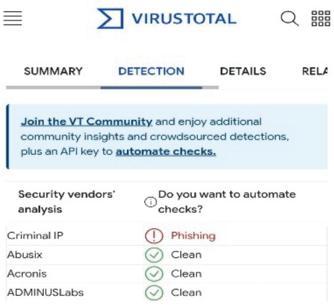
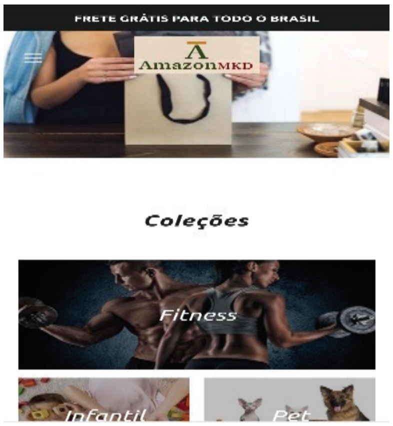
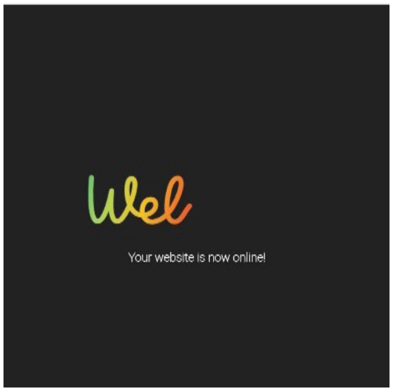
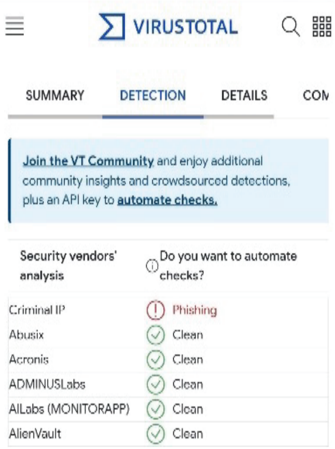
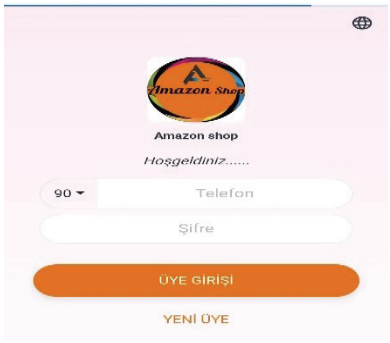
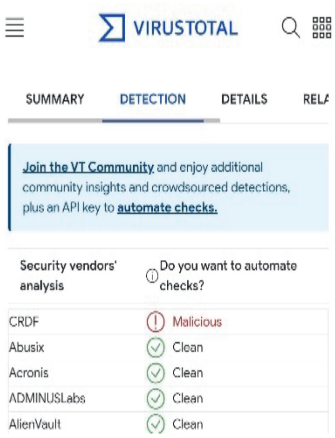
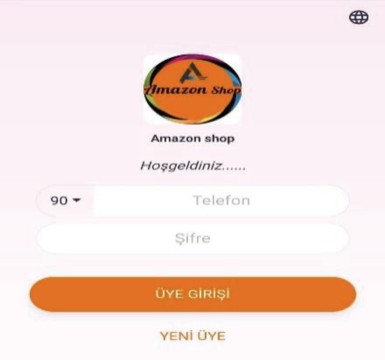
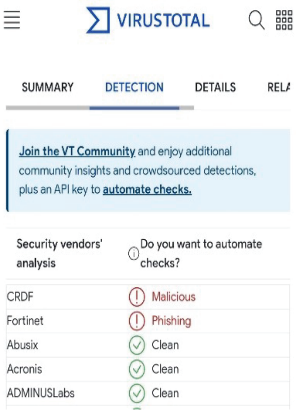
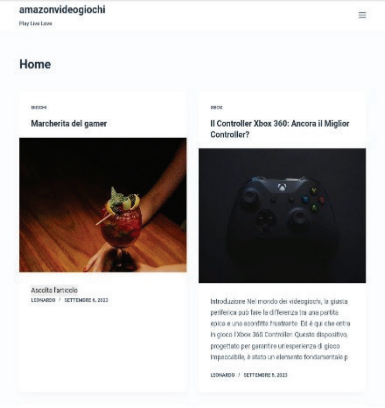
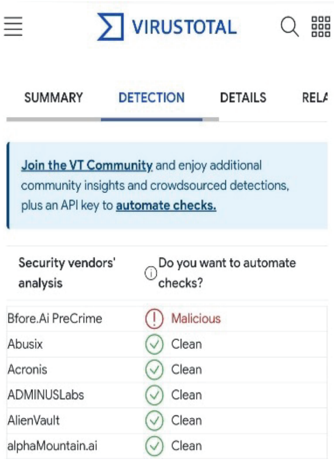
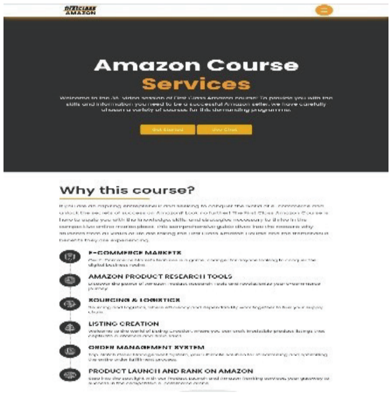
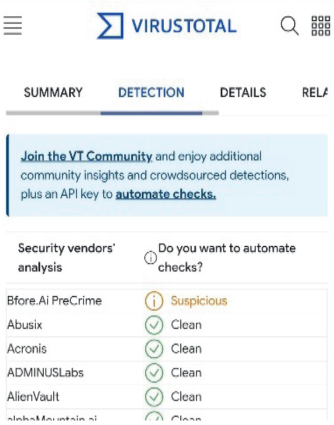
Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
8	Update-microsoft.link (Redirect to https://update-microsoft.link/)  Web server is down Error code 521 Visit cloudflare.com for more information. 2023-09-09 10:40:39 UTC You Browser Working Marseille Cloudflare Working update-microsoft.link Host Error	3 security vendors flagged this URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS LINK Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis / Do you want to automate checks? BitDefender – Phishing G-Data – Phishing alphaMountain.ai – Suspicious Abusix – Clean Acronis – Clean ADMINUSLabs – Clean AICC (MONITORAPP) – Clean AlienVault – Clean Antiy-AVL – Clean	Connected IPs: 1 Main IP: 2606:4700:3037::ac43:c4cd Connected domains: 1 Connected countries: 1 HTTP transactions: 7 Location: United States Registrant: CLOUDFLAREN-ET, US Registrar: ARIN, LLC

TABLE IX

Suspicious look-alike Domains of Amazon

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
1.	amazoncashclaim.org (Redirects to https://beacons.ai/)  Beacons's Top Creator Agencies 2023 is out now! → Beacons Login Sign up The most powerful link in bio. Plus so much more. Build your creator store. Score brand deals. Own and grow your audience. All from a Beacons link in bio. Get Started 505,999 100 Join millions of creators making it on Beacons coffeebae97 Influencer · Jewel Singer Songwriter · Alanis Morissette Singer Songwriter · NOM_Life Food Creators · Tokyo Treat Japanese Snacks · frankniu Tech Influencer · Claudia Leitte Brazilian Singer	2 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS CON Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis / Do you want to automate checks? Bfore.Ai PreCrime – Malicious BitDefender – Phishing G-Data – Phishing Abusix – Clean Acronis – Clean	Connected IPs: 33 Main IP: 2606:4700:10::6816:2662 Connected domains: 25 Connected countries: 2 HTTP transaction: 221 Location: United States Registrar: Marcaria to CLOUDFLAR-ENET, US Created on: 16 December, 2017
2.	Amazongd.com (Redirects to https://amazongd.com/) 	1 security vendor flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis / Do you want to automate checks? Criminal IP – Phishing Abusix – Clean Acronis – Clean ADMINUSLabs – Clean	Connected IPs: 9 Main IP: 199.26.84.165 Connected domains: 7 Connected countries: 2 HTTP transaction: 121 Location: United States Registrant: DFW-DATACENTER, US. Registrar: NameSilo, LLC Created on: August 24th, 2023

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
3.	Amazonmkd.com (Redirects to https://amazonmkd.com/)  FRETE GRÁTIS PARA TODO O BRASIL AmazonMKD Coleções Fitness Infantil Pet	No security vendors flagged this URL as malicious	Connected IPs: 3 Main IP: 23.227.38.32 Connected domains: 3 Connected countries: 2 HTTP transaction: 50 Location: Ottawa, Canada Registrant: CLOUDFLARENET, US. Registrar: ARIN, LLC
4.	Amazonpalletliquidation.com Redirects to http://amazonpalletliquidation.com/)  	No security vendors flagged this URL as malicious  Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Criminal IP ⓘ Phishing Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AILabs (MONITORAPP) ✓ Clean AlienVault ✓ Clean	Connected IPs: 5 Main IP: 173.252.167.20 Connected domains: 5 Connected countries: 2 HTTP transaction: 6 Location: Wilmington United States Registrant: ORANGEHOST, US. Registrar: Wild West Domain, LLC Created on: July 22nd, 2023
5.	Amazonshop.one (Redirects to https://amazonshop.one/index/user/login.html)  Amazon Shop Amazon shop Hoşgeldiniz...... 90 Telefon Şifre ÜYE GIRIŞI YENI ÜYE	1 security vendor flagged this URL as malicious.  Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? CRDF ⓘ Malicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AlienVault ✓ Clean	Connected IPs: 3 Main IP: 2a06:98c1:3120::3 Connected domains: 3 Connected countries: 2 HTTP transaction: 26 Location: United States Registrant: CLOUDFLARENET, US Registrar: NameSilo, LLC Created on: July 23rd, 2023

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
6.	Amazonshop.work (Redirects to https://amazonshop.work/index/user/login.html)  Amazon Shop Amazon shop Hoşgeldiniz...... 90 ▾ Telefon Şifre ÜYE GİRİŞİ YENİ ÜYE	2 security vendors flagged this URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? CRDF ⓘ Malicious Fortinet ⓘ Phishing Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean	Connected IPs: 3 Main IP: 2606:4700:3037::6815:57cb Connected domains: 3 Connected countries: 2 HTTP transaction: 26 Location: United States Registrant: CLOUDFLARENET, US Registrar: ARIN, LLC
7.	amazonvideogiochi.com Redirects to https://amazonvideogiochi.com/)  amazonvideogiochi Play Live Love Home GIOCHI Marcherita del gamer Ascolta l'articolo LEONARDO / SETTEMBRE 6, 2023 XBOX Il Controller Xbox 360: Ancora il Miglior Controller? Introduzione Nel mondo dei videogiochi, la giusta periferica può fare la differenza tra una partita epica e una sconfitta frustrante. Ed è qui che entra in gioco l'Xbox 360 Controller. Questo dispositivo, progettato per garantire un'esperienza di gioco impeccabile, è stato un elemento fondamentale p LEONARDO / SETTEMBRE 5, 2023	1 security vendor flagged this URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Bfore.Ai PreCrime ⓘ Malicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AlienVault ✓ Clean alphaMountain.ai ✓ Clean	Connected IPs: 3 Main IP: 35.227.194.51 Connected domains: 3 Connected countries: 2 HTTP transaction: 28 Location: Kansas City, United States Registrant: GOOGLE, US Registrar: TUCOWS, INC
8.	firstclassamazon.com (Redirects to http://firstclassamazon.com/)  FIRSTCLASS AMAZON Amazon Course Services Why this course? E-COMMERCE MARKETS AMAZON PRODUCT RESEARCH TOOLS SOURCING & LOGISTICS LISTING CREATION ORDER MANAGEMENT SYSTEM PRODUCT LAUNCH AND RANK ON AMAZON	No security vendors flagged this URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Bfore.Ai PreCrime ⓘ Suspicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AlienVault ✓ Clean alphaMountain.ai ✓ Clean	Connected IPs: 7 Main IP: 64.20.34.139 Connected domains: 6 Connected countries: 3 HTTP transaction: 96 Location: United States Registrant: IS-AS-1, US Registrar: Internet Domain Service BS Corp. Created on: July 17th 203.

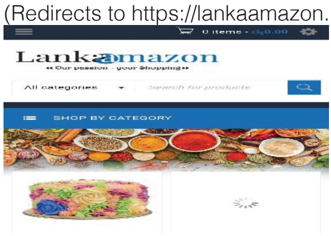
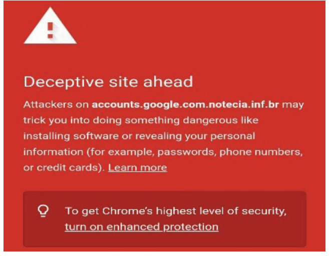
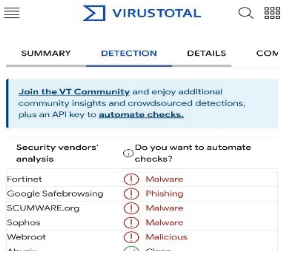
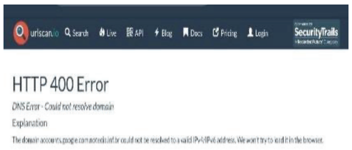
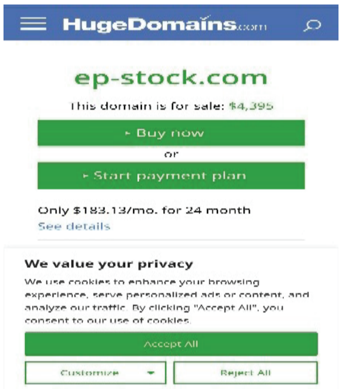
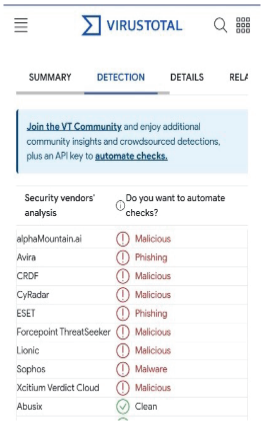
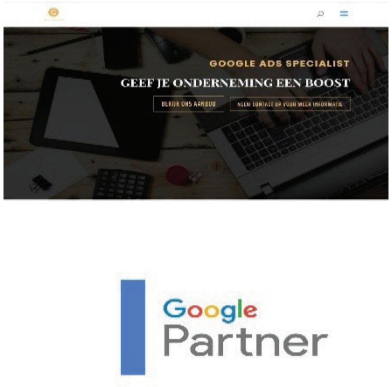
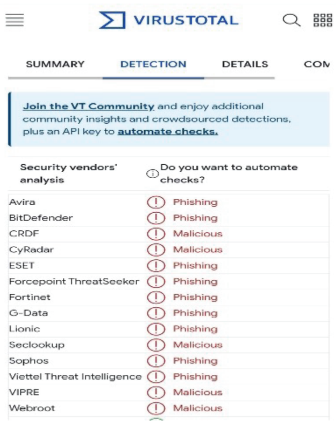
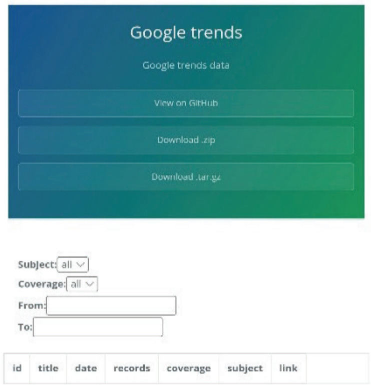
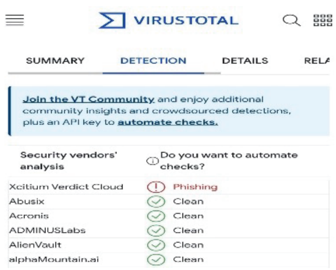
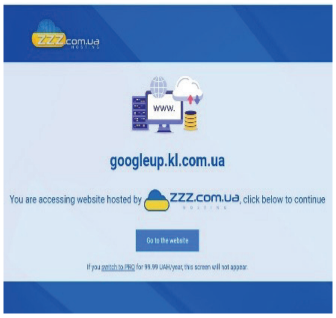
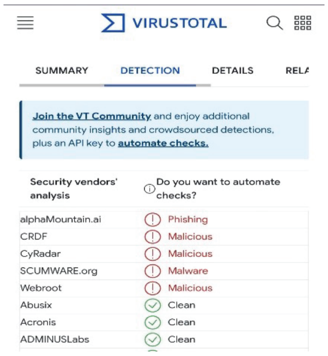
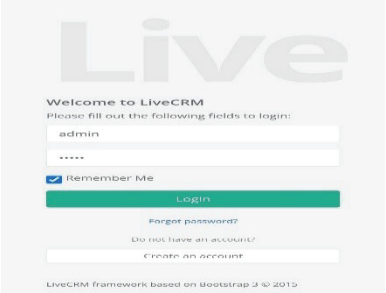
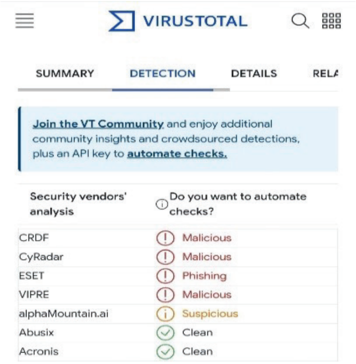
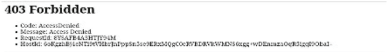
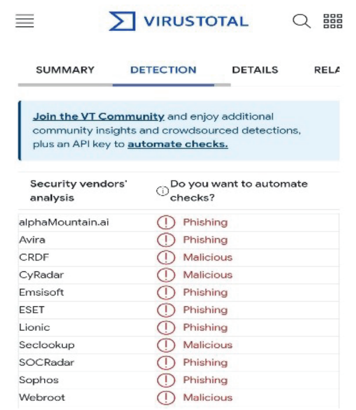
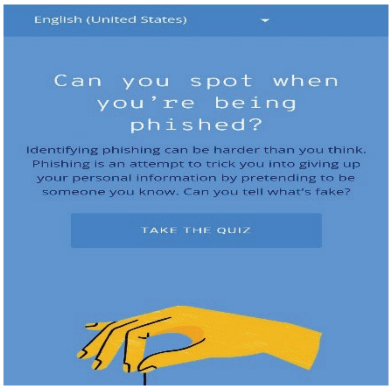
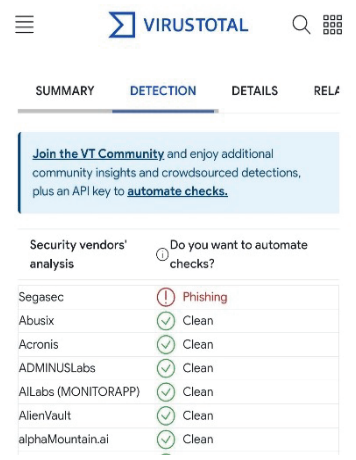
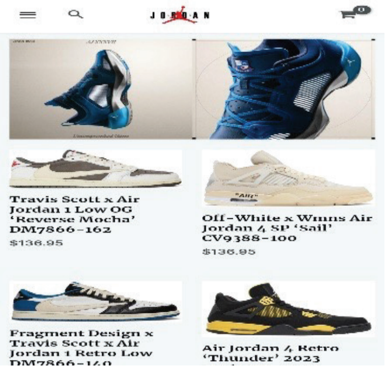
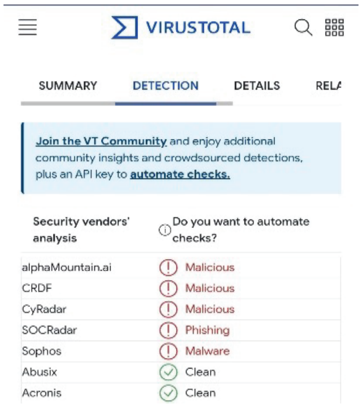
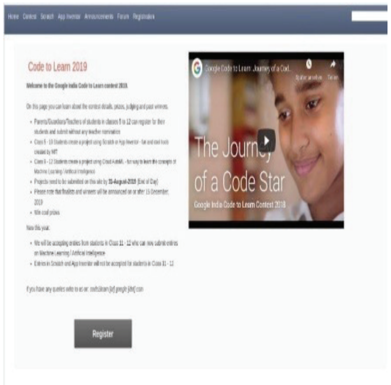
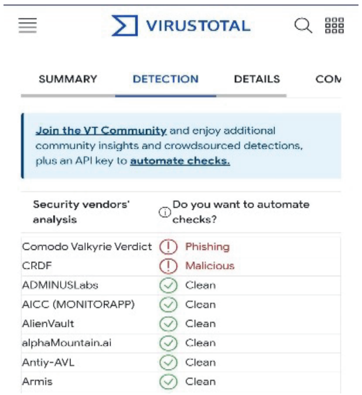
Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
9.	lankaamazon.lk (Redirects to https://lankaamazon.lk/)  0 items - රු0.00 Lankaamazon « Our passion - your Shopping » All categories Search for products SHOP BY CATEGORY	No security vendors flagged this URL as malicious.	Connected IPs: 8 Main IP: 209.133.218.106 Connected domains: 7 Connected countries: 2 HTTP transaction: 88 Location: Tampa, United States Registrant: HVC-AS, US Registrar: ARIN
10.	primeamazonreviews.com (Redirects to https://primeamazonreviews.com) Amazon Prime's Hottest Deals and Reviews Coming Soon A faster, better and easier way to choose	No security vendors flagged this domain as malicious.	Connected IPs: 6 Main IP: 192.0.78.24 Connected domains: 4 Connected countries: 2 HTTP transaction: 23 Location: San Francisco, United States Registrant: AUTOMATTIC, US. Registrar: Automattic Inc. Created on: July 23rd 2023.

TABLE X
Suspicious look-alike Domains of Google

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
1.	Accounts.google.com.notecia.inf.br (Redirects to http://accounts.google.com.notecia.inf.br/)  Deceptive site ahead Attackers on **accounts.google.com.notecia.inf.br** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more To get Chrome's highest level of security, turn on enhanced protection	5 security vendors flagged this URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS COM Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Fortinet ⓘ Malware Google Safebrowsing ⓘ Phishing SCUMWARE.org ⓘ Malware Sophos ⓘ Malware Webroot ⓘ Malicious	No Report.  urlscan.io Search Live API Blog Docs Pricing Login SecurityTrails HTTP 400 Error *DNS Error - Could not resolve domain* Explanation The domain accounts.google.com.notecia.inf.br could not be resolved to a valid IPv4/IPv6 address. We won't try to load it in the browser.
2.	Google.open.pdf.ep-stock.com (Redirects to https://www.hugedomains.com/domain_profile.cfm?d=ep-stock.com)  HugeDomains.com ep-stock.com This domain is for sale: $4,395 ▸ Buy now or ▸ Start payment plan Only $183.13/mo. for 24 month See details We value your privacy We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Accept All Customize ▾ Reject All	9 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? alphaMountain.ai ⓘ Malicious Avira ⓘ Phishing CRDF ⓘ Malicious CyRadar ⓘ Malicious ESET ⓘ Phishing Forcepoint ThreatSeeker ⓘ Malicious Lionic ⓘ Malicious Sophos ⓘ Malware Xcitium Verdict Cloud ⓘ Malicious Abusix ✓ Clean	Connected IPs: 8 Main IP: 85.17.175.148 Connected domains: 4 Connected countries: 2 HTTP transaction: 10 Location: Netherlands Registrant: LEASEWEB-NL-AMS-01 Netherlands, NL Registrar: TurnCommerce, Inc. DBA NameBright.com. Created on: October 26th 2014 Urlscan.io Verdict: Potentially Malicious

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
3.	googleadsrotterdam.com (Redirects to https://googleadsrotterdam.com/  GOOGLE ADS SPECIALIST GEEF JE ONDERNEMING EEN BOOST BEKIJK ONS AANBOD NEEM CONTACT OP VOOR MEER INFORMATIE Google Partner	14 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS COM Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Avira ⓘ Phishing BitDefender ⓘ Phishing CRDF ⓘ Malicious CyRadar ⓘ Malicious ESET ⓘ Phishing Forcepoint ThreatSeeker ⓘ Phishing Fortinet ⓘ Phishing G-Data ⓘ Phishing Lionic ⓘ Phishing Seclookup ⓘ Malicious Sophos ⓘ Phishing Viettel Threat Intelligence ⓘ Phishing VIPRE ⓘ Malicious Webroot ⓘ Malicious	Connected IPs: 1 Main IP: 185.56.146.228 Connected domains: 1 Connected countries: 1 HTTP transaction: 6 Location: Netherlands Registrant: SERVERIUS-AS, NL Registrar: Hostinger, UAB Created on: August 23rd 2018 Urlscan.io Verdict: Potentially Malicious
4.	googlefoundation.somee.com (Redirects to http://googlefoundation.somee.com/)	2 detected files embedding this domain	Connected IPs: 1 Main IP: 185.199.108.153 Connected domains: 1 Connected countries: 1 HTTP transaction: 1 Location: Dallas, United States Registrant: JOESDATACENTER, US Registrar: ARIN
5.	googletrends.github.io (Redirects to http://googletrends.github.io/)  Google trends Google trends data View on GitHub Download .zip Download .tar.gz Subject: all Coverage: all From: To: id title date records coverage subject link	1 security vendor flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Xcitium Verdict Cloud ⓘ Phishing Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean AlienVault ✓ Clean alphaMountain.ai ✓ Clean	Connected IPs: 6 Main IP: 192.0.78.24 Connected domains: 6 Connected countries: 2 HTTP transaction: 12 Location: United States Registrant: FASTLY, US Registrar: ARIN
6.	Googleup.kl.com.ua (Redirects to http://googleup.kl.com.ua/)  ZZZ.com.ua HOSTING www. googleup.kl.com.ua You are accessing website hosted by ZZZ.com.ua HOSTING, click below to continue Go to the website If you switch to PRO for 99.99 UAH/year, this screen will not appear.	5 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? alphaMountain.ai ⓘ Phishing CRDF ⓘ Malicious CyRadar ⓘ Malicious SCUMWARE.org ⓘ Malware Webroot ⓘ Malicious Abusix ✓ Clean Acronis ✓ Clean ADMINUSLabs ✓ Clean	Connected IPs: 5 Main IP: 95.211.16.66 Connected domains: 3 Connected countries: 2 HTTP transaction: 11 Location: Den Haag, Netherlands Registrant: LEASEWEB-NL-AMS-01 Netherlands, NL Registrar: RIPENCC Urlscan.io Verdict: Potentially Malicious

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
7.	Googlewale.com (Redirects to https://googlewale.com/livecrm/web/index.php?r=site%2Flogin)  Live Welcome to LiveCRM Please fill out the following fields to login: admin ••••• ☑ Remember Me Login Forgot password? Do not have an account? Create an account LiveCRM framework based on Bootstrap 3 © 2015	5 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis — Do you want to automate checks? CRDF: Malicious CyRadar: Malicious ESET: Phishing VIPRE: Malicious alphaMountain.ai: Suspicious Abusix: Clean Acronis: Clean	Connected IPs: 3 Main IP: 108.181.162.229 Connected domains: 3 Connected countries: 2 HTTP transaction: 38 Location: Dallas, United States Registrant: AS40676, US Registrar: GoDaddy.com, LLC Created on: November 30th 2016
8.	Numbers-google.com (Redirects to https://numbers-google.com/)  403 Forbidden • Code: AccessDenied • Message: Access Denied • RequestId: 8YSAFB4A3HTJY94M • HostId: 6oKgzhBj4cNTI9tVHbrJnPpp8n3se9ERxMQgC0cRVBDRVkWMN56xgg+wDEnmzaOqR5lgqI9Obal-	11 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis — Do you want to automate checks? alphaMountain.ai: Phishing Avira: Phishing CRDF: Malicious CyRadar: Malicious Emsisoft: Phishing ESET: Phishing Lionic: Phishing Seclookup: Malicious SOCRadar: Phishing Sophos: Phishing Webroot: Malicious	Connected IPs: 4 Main IP: 13.225.87.59 Connected domains: 4 Connected countries: 2 HTTP transaction: 229 Location: Seattle, United States Registrant: AMAZON-02, US Registrar: Amazon Registrar, Inc. Created on: May 16th 2018 Urlscan.io Verdict: Potentially Malicious
9.	Phishingquiz.withgoogle.com (Redirects to https://phishingquiz.withgoogle.com/)  English (United States) Can you spot when you're being phished? Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake? TAKE THE QUIZ	1 security vendor flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis — Do you want to automate checks? Segasec: Phishing Abusix: Clean Acronis: Clean ADMINUSLabs: Clean AILabs (MONITORAPP): Clean AlienVault: Clean alphaMountain.ai: Clean	Connected IPs: 5 Main IP: 172.253.118.141 Connected domains: 5 Connected countries: 1 HTTP transaction: 20 Location: United States Registrant: GOOGLE, US Registrar: ARIN

Sr. No.	Suspicious look-alike domain	Virus Total Report	Urlscan.io Report
10.	shoesgoogle.com (Redirects to https://www.shoesgoogle.com/)  JORDAN Travis Scott x Air Jordan 1 Low OG 'Reverse Mocha' DM7866-162 $136.95 Off-White x Wmns Air Jordan 4 SP 'Sail' CV9388-100 $136.95 Fragment Design x Travis Scott x Air Jordan 1 Retro Low DM7866-140 Air Jordan 4 Retro 'Thunder' 2023	5 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS RELA Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? alphaMountain.ai Malicious CRDF Malicious CyRadar Malicious SOCRadar Phishing Sophos Malware Abusix Clean Acronis Clean	Connected IPs: 5 Main IP: 2a06:98c1:3121::3 Connected domains: 5 Connected countries: 3 HTTP transaction: 68 Location: United States Registrant: CLOUDFLARENET, US Registrar: ARIN.
11.	codetolearn.withgoogle.com (Redirects to https://codetolearn.withgoogle.com/)  Home Contest Scratch App Inventor Announcements Forum Registration Code to Learn 2019 Welcome to the Google India Code to Learn contest 2019. On this page you can learn about the contest details, prizes, judging and past winners. • Parents/Guardians/Teachers of students in classes 5 to 12 can register for their students and submit without any teacher nomination • Class 5 - 10 Students create a project using Scratch or App Inventor - fun and cool tools created by MIT • Class 11 - 12 Students create a project using Cloud AutoML - fun way to learn the concepts of Machine Learning / Artificial Intelligence • Projects need to be submitted on this site by 31-August-2019 (End of Day) • Please note that finalists and winners will be announced on or after 15 December, 2019 • Win cool prizes New this year: • We will be accepting entries from students in Class 11 - 12 who can now submit entries on Machine Learning / Artificial Intelligence • Entries in Scratch and App Inventor will not be accepted for students in Class 11 - 12 If you have any queries write to us at: codtolearn [at] google [dot] com Google Code to Learn: Journey of a Cod... The Journey of a Code Star Google India Code to Learn Contest 2018 Register	2 security vendors flagged the redirected URL as malicious.  VIRUSTOTAL SUMMARY DETECTION DETAILS COM Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks. Security vendors' analysis ⓘ Do you want to automate checks? Comodo Valkyrie Verdict Phishing CRDF Malicious ADMINUSLabs Clean AICC (MONITORAPP) Clean AlienVault Clean alphaMountain.ai Clean Antiy-AVL Clean Armis Clean	Connected IPs: 6 Main IP: 2a00:1450:4001:808::2011 Connected domains: 3 Connected countries: 1 HTTP transaction: 22 Location: Frankfurt am Main, Germany Registrant: GOOGLE – Google LLC, US Registrar: ARIN.

IV. Discussion

After examining 10 websites and using dnstwist to identify 1598 registered look-alike domains, we found 13 types of permutations, with the most common being addition, homoglyph, insertion, and replacement. This led to the discovery of 231 suspicious websites, of which 118 were reachable. Notably, 49% of these registered look-alike domains were inaccessible, while 51% were operational. These findings align with a study by Frischknecht et al. in 2021 [3] that found 48% of such domains remained unused. In a study by Peng et al. in 2021 [15], VirusTotal flagged 50% of globally accessible websites which were identified by dnstwist as malicious, while domestic websites were not labeled as such. The study observed that deceptive domains, resembling legitimate ones with a resemblance range of 30% to 98%, consistently redirected users back to the genuine domains. Similar findings were also observed in a review by Varshney et al. in 2016 [16], where analysis techniques designed for the detection of phishing websites were discussed. The use of fuzzy hashes generated from site HTML content to detect potential phishing webpages, as well as the identification of mail servers used by deceptive domains, was successfully carried out with dnstwist. This aligns with previous studies by Prasad in 2022 [17] that highlighted dnstwist's value in spotting deceptive domains and determined the total count of blacklisted domains through the identification of typo variants using dnswist. The similarity indicates the correctness and accuracy of the tool used. The study using OpenSquat identified a total of 155,298 domains from five sample websites. Among them, 103 were engaged in domain squatting, making it the biggest number of active phishing websites at 960, and 53 domains had suspicious certificates. OpenSquat also pinpointed six websites with a high confidence level in webpage similarity and supported various squatting techniques. These findings are consistent with research by Frischknecht et al. in 2021 [3], which highlighted OpenSquat's effectiveness in identifying look-alike domains. The VirusTotal report indicated that various vendors flagged the squatted domains, active phishing websites, and websites with suspicious certificates as malicious and phishing-related. The analysis report of Urlscan.io provided valuable findings such as the domains' associated IP addresses, geographical location of domain operation, registrar information, registrant details, UrlScan verdict, and the date of domain creation of the look-alike domains detected by dnstwist and OpenSquat. The geographic location indicated that most look-alike websites were hosted in the United States and Germany. According to a study conducted by Zingerle in 2016 [18], the biggest number of look-alike websites were found in the United Kingdom (220), followed by the United States (163), and the United Arab Emirates (35). In 2021, Frischknecht et al. [3] discovered that a significant number of look-alike domains appeared to be hosted by a limited number of domain parking services, such as Sedo and GoDaddy. However, our study revealed that the look-alike domains we examined were hosted by various registrars, with ARIN (American Registry for Internet Numbers) and GoDaddy.com being the most frequently utilized services.

V. Conclusion and Future Work

The study thoroughly examined the deceptive domains and compared them to the original domains, assessing their potential maliciousness using services like VirusTotal, urlscan.io, and Alienvault. The focus extended to scrutinizing suspicious mail servers and name servers, emphasizing the financial incentive for cyber squatters who exploit these domains for profit or fraudulent activities. The research offers a practical approach for combating cybersquatting attacks, homograph attacks, online fraud, and phishing, highlighting the importance of proactive website monitoring for organizations to protect themselves and their customers.

In this study, we concentrated on detecting lookalike domains by harnessing the power of open-source tools. Through these tools, we obtained intricate details on all registered lookalike domains. Additionally, we employed online cyber security services to distinguish malicious domains from the registered pool. This methodology doesn't provide only comprehensive insights for the domain ecosystem but also facilitates precise threat identification, thereby contributing to enhanced cyber security measures. While our current proposed techniques are simple and cost-effective, incorporating advanced algorithms and machine learning models would significantly enhance our methodology, offering further improvements.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

Acknowledgement

We would like to express our appreciation to our friends for their technical assistance during the completion of this research. Their support and generosity ensured that we had the necessary tools and resources to carry out our research effectively.

References

[1] S. Wright, "Cybersquatting at the intersection of internet domain names and trademark law," IEEE Communications Surveys & Tutorials, pp. 193-205, 2010.

[2] C. Gasimova, "Domain name and trademark infringement (Cybersquatting) in the digital age," Available via SSRN 434489, pp. 4-5, 2022.

[3] P. Frischknecht, O. Nierstrasz and P. Gadient, "Detection of Cybersquatted Domains," Software Composition Group

Institute for Computer Science, pp. 4-15, 2021.

[4] J. Spaulding, S. Upadhyaya and A. Mohaisen, “The landscape of domain name typo squatting: Techniques and countermeasures,” 11th International Conference on Availability, Reliability and Security (ARES), pp. 284-289, 2016.

[5] A. Khormali, “Domain name system security and privacy: A contemporary survey,” Computer Networks, pp. 185, 2021.

[6] S. Deo, “Cybersquatting: Threat to domain name,” International Journal of Innovative Technology and Exploring Engineering, pp. 1432-1434, 2019.

[7] R. Fouchereau, and K. Rychkov, Global DNS Threat Report Understanding the Critical Role of DNS in Network Security, 2019.

[8] E George, “Key Takeaways from the 2023 Domain Impersonation Report,” [online]

[9] Available:https://www.tripwire.com/state-of-security/key-takeaways-2023-domain-impersonation-report, 2023.

[10] B. Grétarsson, I. Sigurðsson and S. Sigurðsson, “Dumbainhunter 2.0: Hunting malicious domains,” Thesis of 12 ECTS, pp. 7-22, 2020.

[11] R. Masri and M. Aldwairi, “Automated malicious advertisement detection using virustotal, urlvoid, and trendmicro,” 2017 8th International Conference on Information and Communication Systems (ICICS), pp. 336-341, 2017.

[12] J. Okesola, S. Afolakemi, A. Owoade, “Malvertisements Detection using urlscan.Io, Pulsedive, and SucuriSiteCheck,” 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG), pp. 1-8, 2023.

[13] J. Bowling, “Alienvault: the future of security information management,” 2010 Linux Journal, 2010.

[14] Elceef, Dnstwist, [online] Available: https://github.com/elceef//dnstwist. [Accessed May 22, 2023].

[15] Atenreiro, Opensquat, [online] Available: https://github.com/atenreiro/opensquat. [Accessed May 21, 2023].

[16] P. Peng, L. Yang and L. Song, “Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines,” Proceedings of the Internet Measurement Conference, pp. 478-485, 2019.

[17] G. Varshney, M. Mishra and P.K. Atrey, “A survey and classification of web phishing detection schemes,” Security and Communication Networks 9 (18), pp. 6266-6284, 2016.

[18] A. Prasad, “Investigating whether typosquatting targets children,” University of Twente, pp. 6-12, 2022.

[19] A. Zingerle, “Trust Us and Our Business Expands! How Net-activists Take Down Fraudulent Business Websites,” [online] Available: http://2016.xcoax.org, 2016.