WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Revelations on Eevilcorp

Table of Contents

Executive Report

Phishing, despite its age and infamy, remains one of the top threats to corporate and personal networks alike. And it's not hard to see why—it continues to be effective. In fact, more than a third of all data breaches today involve phishing.

It's also been said that art imitates life. In the cybersecurity world, though, the opposite could also be true. So, if you think E Corp, short for "Evil Corp," only exists in the TV show "Mr. Robot," think again. A phishing group known as "Eevilcorp" has been wreaking havoc among organizations and individuals worldwide.

Vade's Threat Intelligence and Response Center (TIRC) researchers analyzed what they dubbed the "Eevilcorp phishing campaign" and the malware its perpetrators used in depth. They identified nine domains and subdomains as IoCs, namely:

- periodic-checker[.]glitch[.]me
- scan-verified[.]glitch[.]me
- transfer-with[.]glitch[.]me
- air-dropped[.]glitch[.]me
- precise-share[.]glitch[.]me
- monthly-payment-invoice[.]glitch[.]me
- monthly-report-check[.]glitch[.]me
- eevilcorp[.]online
- ultimotempore[.]online

WhoisXML API researchers expanded the published list of IoCs and uncovered:

- Nine unique IP addresses to which the domains and subdomains identified as IoCs resolved
- 579 domains that shared the IoCs' possibly dedicated hosts, 13 of which were categorized as malicious based on a bulk malware check
- 20 domains that started with the strings **microsoft + outlook** and **adobe + document + cloud**, six of which were classified as malicious by a bulk malware check

- 715 subdomains that contained the strings **microsoft + outlook** and **adobe + document + cloud**, eight of which turned out to be malicious based on a bulk malware check

Eevilcorp IoC Facts

The Vade TIRC researchers discovered that Eevilcorp trailed its sights on at least two big tech products—Microsoft Outlook and Adobe Document Cloud. They also abused the glitch[.]me platform to host seven of their specially crafted subdomains and used two other domains for their ongoing campaign.

We first subjected the nine web properties identified as IoCs to a bulk WHOIS lookup and found that only two had available WHOIS records—eevilcorp[.]online and ultimotempore[.]online. Both were administered by Hostinger Operations, UAB and had redacted WHOIS records, protected by Privacy Protect, LLC. They were relatively newly created, specifically in the first two months of this year and registered in the U.S.

Website categorization lookups for all nine domains also revealed interesting findings shown in the table below.

DOMAIN	WEBSITE CATEGORIZATION LOOKUP RESULT
eevilcorp[.]online	Phishing and other fraud
ultimotempore[.]online	Phishing and other fraud
periodic-checker[.]glitch[.]me	Phishing and other fraud
scan-verified[.]glitch[.]me	Phishing and other fraud
transfer-with[.]glitch[.]me	Phishing and other fraud
air-dropped[.]glitch[.]me	Phishing and other fraud
precise-share[.]glitch[.]me	Phishing and other fraud
monthly-payment-invoice[.]glitch[.]me	Phishing and other fraud
monthly-report-check[.]glitch[.]me	Phishing and other fraud

Eevilcorp IoC Findings

In an effort to determine if organizations and individuals need to steer clear of web properties other than those that have already been identified as Eevilcorp IoCs, we expanded the current list aided by DNS intelligence.

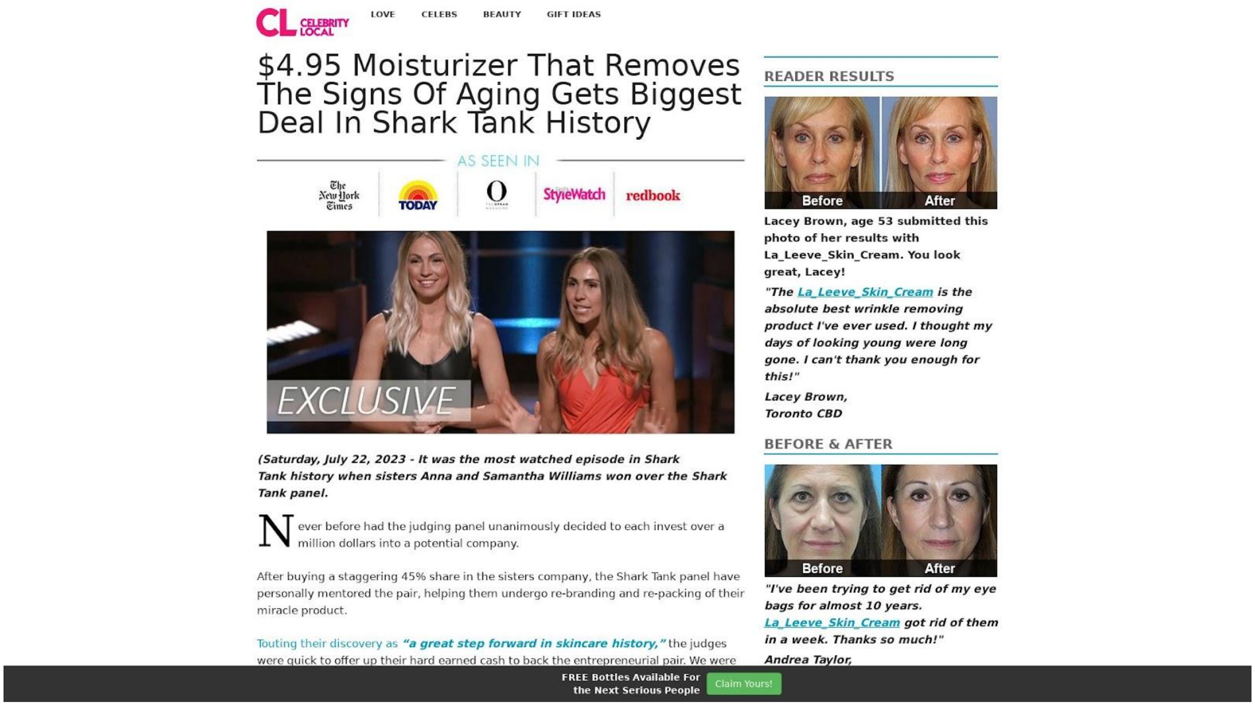
In total, the IoCs resolved to nine unique IP addresses. Only eight of them, however, had retrievable A records based on a bulk IP geolocation lookup. The result also revealed that four were administered by Amazon and the remaining half by Cloudflare. All of the resolving IP addresses were geolocated in the U.S.

We subjected the IoCs to DNS lookups as well, which revealed that many, particularly those hosted on glitch[.]me, used the same four shared IP hosts—3[.]212[.]249[.]142, 44[.]198[.]62[.]156, 54[.]144[.]28[.]217, and 54[.]235[.]167[.]164.

The remaining four IP addresses were possibly dedicated based on reverse IP lookups, hosting 579 domains in total not on the published list of IoCs. A bulk malware check for the IP-connected domains showed that 13 were malicious.

Five of the 13 malicious domains continued to host live content as evidenced by screenshot lookup results. Two of them proved most interesting in that apart from being detected as malware hosts, their content didn't match what their domain names suggested.

First off, nutritionfactsforfree[.]online hosted what looked like a celebrity news site. Perjakatoto[.]net (perjakatoto is Malay for "girl") and vldb2009[.]org, meanwhile, led to gambling sites.



$4.95 Moisturizer That Removes The Signs Of Aging Gets Biggest Deal In Shark Tank History

(Saturday, July 22, 2023 - It was the most watched episode in Shark Tank history when sisters Anna and Samantha Williams won over the Shark Tank panel.

Never before had the judging panel unanimously decided to each invest over a million dollars into a potential company.

After buying a staggering 45% share in the sisters company, the Shark Tank panel have personally mentored the pair, helping them undergo re-branding and re-packing of their miracle product.

Touting their discovery as ***"a great step forward in skincare history,"*** the judges were quick to offer up their hard earned cash to back the entrepreneurial pair. We were

READER RESULTS

Lacey Brown, age 53 submitted this photo of her results with La_Leeve_Skin_Cream. You look great, Lacey!

"The La_Leeve_Skin_Cream is the absolute best wrinkle removing product I've ever used. I thought my days of looking young were long gone. I can't thank you enough for this!"

Lacey Brown,
Toronto CBD

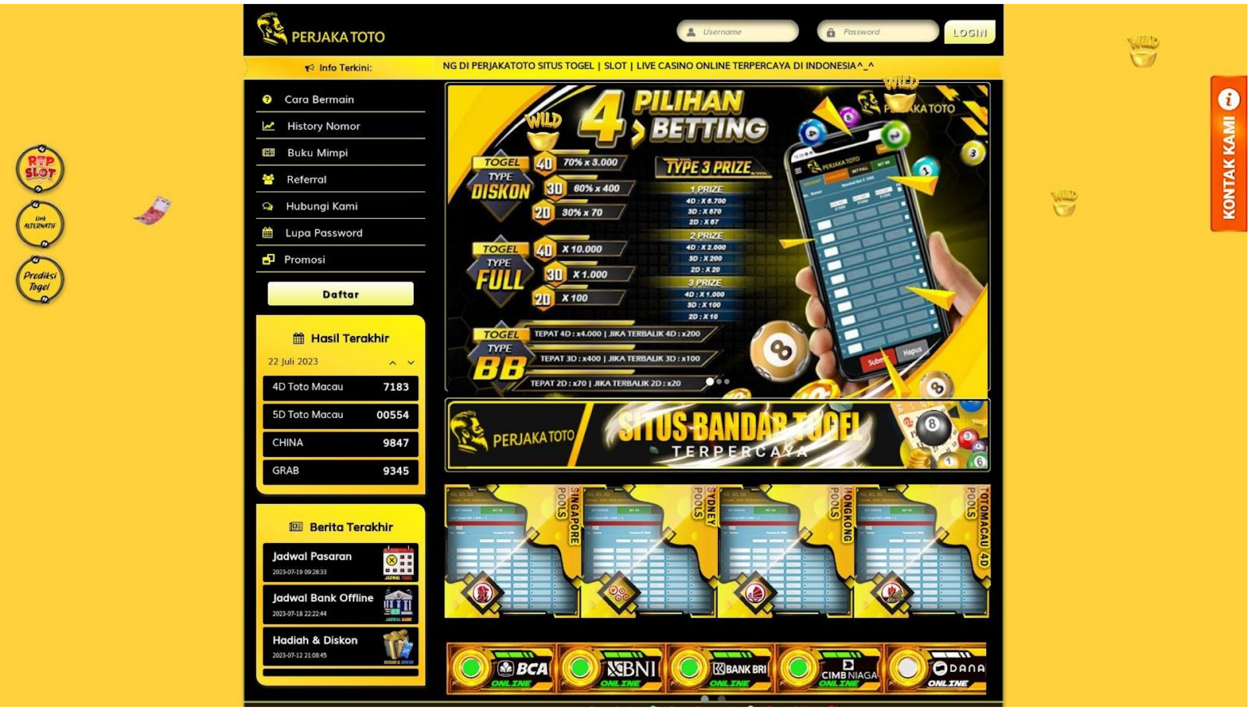
BEFORE & AFTER

"I've been trying to get rid of my eye bags for almost 10 years. La_Leeve_Skin_Cream got rid of them in a week. Thanks so much!"

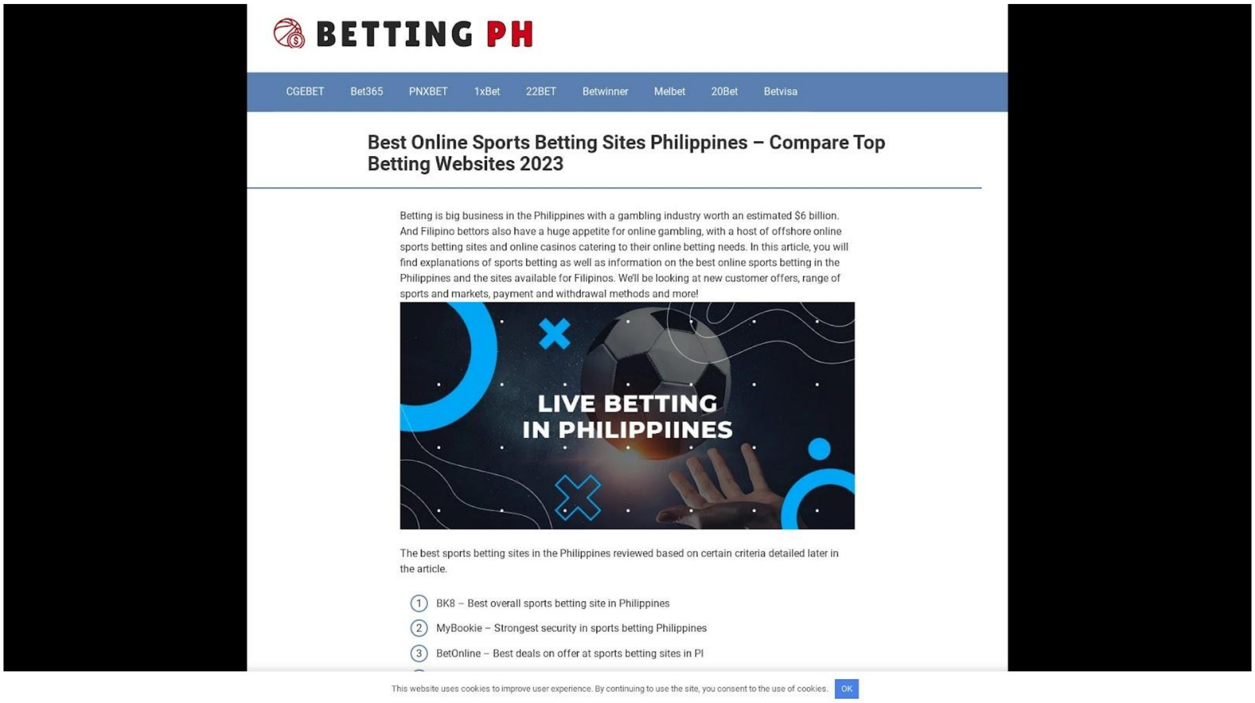
Andrea Taylor,

FREE Bottles Available For the Next Serious People

Screenshot of nutritionfactsforfree[.]online



Screenshot of perjakatoto[.]net



Best Online Sports Betting Sites Philippines – Compare Top Betting Websites 2023

Betting is big business in the Philippines with a gambling industry worth an estimated $6 billion. And Filipino bettors also have a huge appetite for online gambling, with a host of offshore online sports betting sites and online casinos catering to their online betting needs. In this article, you will find explanations of sports betting as well as information on the best online sports betting in the Philippines and the sites available for Filipinos. We'll be looking at new customer offers, range of sports and markets, payment and withdrawal methods and more!

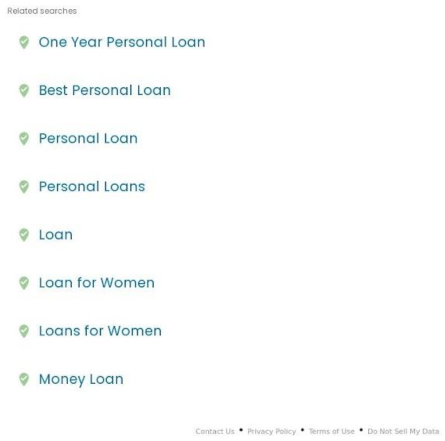
The best sports betting sites in the Philippines reviewed based on certain criteria detailed later in the article.

1. BK8 – Best overall sports betting site in Philippines
2. MyBookie – Strongest security in sports betting Philippines
3. BetOnline – Best deals on offer at sports betting sites in PI

This website uses cookies to improve user experience. By continuing to use the site, you consent to the use of cookies.

Screenshot of vldb2009[.]org

The malicious domain personal-loan-look-seeks[.]today was, on the other hand, truer to its name, as it contained a list of loan-related searches.



Related searches

- One Year Personal Loan
- Best Personal Loan
- Personal Loan
- Personal Loans
- Loan
- Loan for Women
- Loans for Women
- Money Loan

Contact Us • Privacy Policy • Terms of Use • Do Not Sell My Data

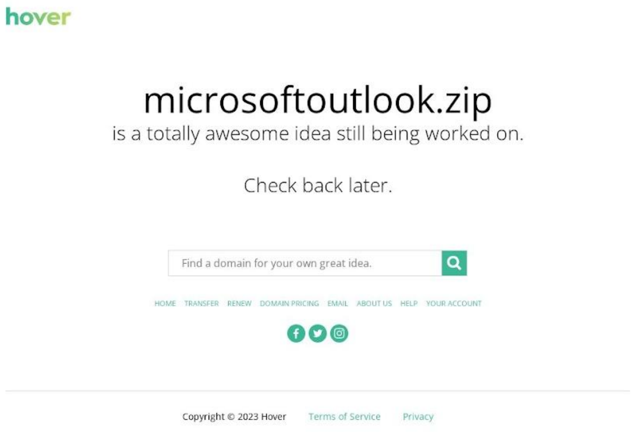
Screenshot of personal-loan-look-seeks[.]today

Next, given the attackers' abuse of popular brands owned by Microsoft and Adobe, we also sought to uncover if they could potentially weaponize other domains and subdomains for future campaigns.

Domains & Subdomains Discovery for domains starting with and subdomains containing **microsoft + outlook** led to the discovery of 20 domains and 715 subdomains created just this year. A similar search for domains starting with and subdomains containing **adobe + document + cloud**, meanwhile, turned up 11 domains and 15 subdomains.

A bulk WHOIS lookup for all the domains we uncovered showed none of them could be publicly attributed to Microsoft and Adobe. None of them shared the registrant email address and other WHOIS details of microsoft[.]com and adobe[.]com.

A bulk malware check for string-connected domains, on the other hand, revealed that six of them were categorized as malicious. While a majority of them were unreachable, one domain led to a site that was, according to its screenshot, under development.



microsoftoutlook.zip

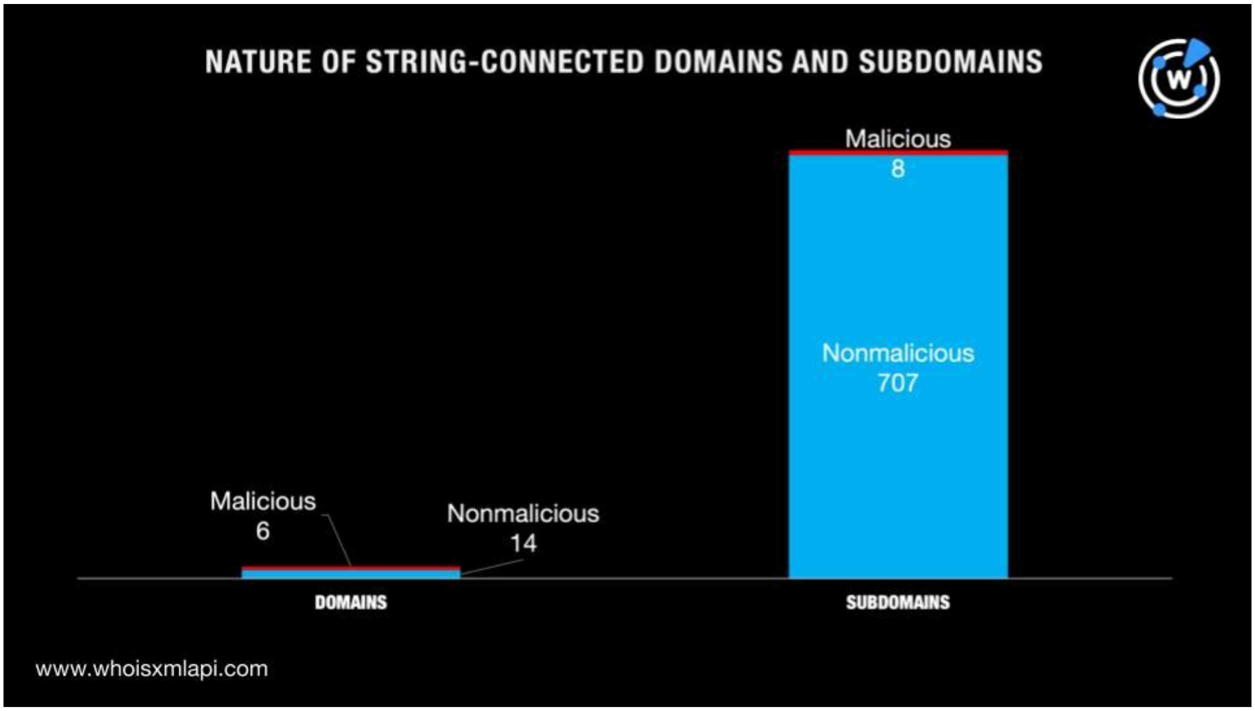
is a totally awesome idea still being worked on.

Check back later.

Copyright © 2023 Hover

Screenshot of microsoftoutlook[.]zip

We also subjected the string-connected subdomains to a bulk malware check, which revealed that eight of them have been detected as malware hosts. Only three of them remained accessible—one led to a blank page while two showed error pages.



—

Our latest foray into the depths of the DNS allowed us to find more digital traces Eevilcorp may have unintentionally left behind. The IoC expansion we performed brought to light more than 1,300 connected properties. Directly related or not to the group's ongoing phishing campaign, the 27 malicious properties we found could pose risks to organizations and individuals alike.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

Sample IoC IP Resolutions

- 104[.]21[.]62[.]191
- 172[.]67[.]138[.]168

- 172[.]67[.]184[.]21
- 104[.]21[.]59[.]213

Sample IP-Connected Domains

- 01server01[.]sbs
- 100seoer[.]com
- 10powerpro[.]club
- 123cendoldawet[.]xyz
- 1bar[.]uk
- 1za8a1q[.]bar
- 2023keeoxezyxaz[.]cyou
- 2biizhug[.]xyz
- 2winph[.]com
- 333tron[.]live
- 3b9n3t1[.]work
- 3y3coin[.]shop
- 4g7ye8[.]cyou
- 4hg333[.]com
- 60ok[.]it
- 637glorietta[.]com
- 69xx1019[.]xyz
- 69xx1671[.]xyz
- 7512289[.]com
- 8crafts[.]cyou
- 96dg[.]in
- 97or3[.]com
- 9se123[.]xyz
- a-prime-drive[.]zone
- actiontreeservicesa[.]com
- actor2athlete[.]com
- addvancestudio[.]com
- adgokanroreva[.]tk
- administrise[.]one
- adriannabialobrzeska[.]pl
- aefr47[.]shop
- agenciab2be[.]com[.]br
- agrcolicener[.]tk
- alassautdusida[.]live
- aljanabdshop[.]com
- allied-esports[.]com
- altukosjaupiccia[.]cf
- aminsamad[.]cf
- amkhatar[.]cf
- ankarapastirma[.]com
- aquavenatus[.]com
- aradiginajans[.]com
- aranex-provider[.]de
- arbbnb[.]net
- architecte[.]asia
- areweeatingfishyfood[.]com
- arirealinon[.]cf
- arshanmedia[.]ir
- artofhome[.]com
- asfwebcamchat[.]ru
- asix88[.]net
- assystengenharia[.]com[.]br
- atasehirdeyim[.]com
- aurumx[.]io
- auswideframeless[.]com[.]au
- avatka[.]ru
- azino777-gv[.]top
- azuremoonstone[.]xyz
- baguette-academy[.]in
- ballspromotion[.]com
- barrettcommunity[.]com
- bbbnoordenveld[.]nl
- bearmtnband[.]com
- benebolton[.]space
- bhaitea[.]sg
- bigcupbrassale[.]com
- bitquickls[.]com
- blazercomaposta[.]icu
- blypw[.]me
- bocoranslotonlinegacor[.]com
- bocphot[.]xyz
- boitier-ethanol[.]net

- bordobet[.]buzz
- bpw2u0[.]cfd
- brain2train[.]net
- brandtchiroclinic[.]com
- brunflohus4[.]com
- bubbelsenjets[.]nl
- bubblegumheaven[.]com
- budget-locksmith-albuquerque[.]com
- buildengineers[.]com
- bulgariangambler[.]com
- buxtonshop[.]com
- buywithccm[.]com
- calivaria[.]org
- campingartikel-neu[.]com
- carshowsigns[.]com
- casapestera[.]ro
- cashofferli[.]com
- cashup[.]me
- cddgc63[.]top
- cemmaresme[.]com
- cen95996[.]com
- centralestagio[.]com
- ceyokahealth[.]com
- chinapo[.]org
- chinesedreamsisgone[.]com
- chloesavageembroidery[.]com
- circuscasino[.]rs
- citizenshipcourtesy[.]cn

Sample Malicious IP-Connected Domains

- mpsconsultingcorp[.]com
- nutritionfactsforfree[.]online
- perjakatoto[.]net
- personal-loan-look-seeks[.]today
- tamilprint23[.]bio
- vldb2009[.]org
- wecindia[.]in

Sample String-Connected Domains

- microsoftoutlook[.]cn
- microsoftoutlook[.]zip
- microsoft365outlook[.]de
- microsoftoutlook[.]com[.]de
- microsoftoutlookonline[.]xn--ngbrx
- adobedocumentscloud[.]ml
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com
- adobedocumentscloud[.]tk
- adobe-documentscloud[.]ml
- adobe-documentscloud[.]cf

Sample Malicious String-Connected Domains

- microsoftoutlook[.]zip
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com

Sample String-Connected Subdomains

- microsoftoutlook[.]com[.]xyz
- microsoftoutlook[.]com[.]com
- microsoft-outlook[.]oculusvr[.]com
- microsoft-outlook[.]williamhill[.]com
- microsoft-outlook[.]attcorona[.]com
- microsoft-outlook[.]onelink[.]me

- outlook-microsoft[.]42web[.]io
- microsoft-outlook[.]just-eat[.]co[.]uk
- microsoft-outlook[.]as[.]me
- microsoftoutlooks[.]intactsolutions[.]net
- outlook[.]microsoft[.]user-login[.]online
- microsoft-outlook[.]hitta[.]se
- outlook[.]microsoft[.]techgyaanii[.]com
- microsoft-outlook[.]quizlet[.]com
- microsoft-outlook[.]menulog[.]co[.]nz
- outlook[.]microsoft[.]vdwal[.]xyz
- microsoft-outlook[.]larksuite[.]com
- microsoft-outlook[.]planningcenteronline[.]com
- microsoft-outlook[.]climedo[.]de
- microsoft-outlook[.]verily[.]com
- microsoft-outlook[.]paydiant[.]com
- microsoft-outlook[.]betsson[.]com
- microsoft-outlook[.]wolf-of-wilderness[.]com
- microsoft-outlook[.]syncsketch[.]dev
- microsoft-outlook[.]staging-airtableblocks[.]com
- microsoft-outlook[.]jfrog[.]com
- microsoft-outlook[.]yelp[.]com
- microsoft-outlook[.]nextdoor[.]de
- microsoft-outlook[.]cyna[.]io
- microsoft-outlook[.]unfold[.]com
- microsoft-outlook[.]connxusdemo[.]com
- microsoft-outlook[.]emotient[.]com
- microsoft-outlook[.]smashfly[.]com
- microsoft-outlook[.]twilio[.]com
- microsoft-outlook[.]wistia[.]com
- outlook[.]microsoft[.]integra-group[.]cz
- microsoft-outlook[.]duolingo[.]com
- microsoft-outlook[.]binance[.]com
- microsoft-outlook[.]acuityscheduling[.]com
- microsoft-outlook[.]withgoogle[.]com
- outlook[.]microsoft[.]demstronic[.]com
- microsoft-outlook[.]yelptop100[.]com
- microsoft-outlook[.]snowflakecomputing[.]com
- microsoft-outlook[.]netlify[.]app
- microsoft-outlook[.]recko[.]io
- microsoft-outlook[.]realtime[.]email
- microsoft-outlook[.]miro[.]com
- outlook[.]microsoft[.]sec-line[.]xyz
- microsoft-outlook[.]litix[.]io
- microsoft-outlook[.]vivy[.]com
- adobeclouddocument[.]lpages[.]co
- adobedocumentcloud[.]ormimas[.]com
- adobedocumentcloud[.]aqualunub[.]com
- adobe-document-cloud[.]webflow[.]io
- www[.]adobedocumentcloud[.]aqualunub[.]com
- adobe-document-cloud[.]en[.]mercadopago[.]com[.]pe
- adobe-document-cloud[.]en[.]humio[.]cloud
- adobe-document-cloud[.]en[.]foodpanda[.]my
- adobe-document-cloud[.]en[.]structure[.]app
- adobe-document-cloud[.]en[.]datad0g[.]com
- adobe-document-cloud[.]en[.]foodpanda[.]ph
- adobe-document-cloud[.]en[.]tccalling[.]net

- documentcloud[.]adobe[.]com[.]i[.]edgekey[.]net
- documentcloud-adobe-com-s[.]vpn2[.]aufe[.]edu[.]cn
- adobefreeuserschannel[.]na1experiencecloud[.]documents[.]adobe[.]com
- outlookmicrosoft-la[.]4lima[.]de
- microsoftoutlook[.]id[.]cghub[.]com
- microsoftoutlook[.]nl[.]mongodb[.]com
- microsoftoutlook[.]en[.]tagomi[.]com
- microsoftoutlook[.]de[.]fortnite[.]com
- microsoftoutlook[.]ro[.]tidalhi[.]fi
- outlook[.]microsoft[.]outlook[.]com[.]bogston[.]com
- microsoft-outlook[.]en[.]8x8pilot[.]com
- microsoft-outlook[.]en[.]ncplatform[.]net
- microsoft-outlook[.]nl[.]bolt[.]com
- microsoft-outlook[.]nl[.]fbsbx[.]com
- microsoft-outlook[.]en[.]affinity[.]co
- microsoft-outlook[.]en[.]netlify[.]app
- microsoft-outlook[.]nl[.]animalfriends[.]co[.]uk
- microsoft-outlook[.]nl[.]8x8pilot[.]com
- microsoft-outlook[.]nl[.]32red[.]com
- microsoft-outlook[.]th[.]canvaslms[.]com
- microsoft-outlook[.]nl[.]climedo[.]de
- microsoft-outlook[.]nl[.]miro[.]com
- microsoft-outlook[.]en[.]cloudinary[.]com
- microsoft-outlook[.]en[.]hitta[.]se
- microsoft-outlook[.]nl[.]caesars[.]com
- microsoft-outlook[.]en[.]claiming[.]com[.]au
- microsoft-outlook[.]en[.]nextdoor[.]nl
- microsoftoutlook1337[.]zendesk[.]com
- microsoft-outlook[.]nl[.]exploretock[.]com
- microsoft-outlook[.]en[.]guildwars2[.]com
- microsoft-outlook[.]en[.]staging-airtableblocks[.]com
- microsoft-outlook[.]en[.]shopkeep-staging[.]com
- microsoft-outlook[.]en[.]goodrx[.]com
- microsoft-outlook[.]en[.]fortnite[.]com
- microsoft-outlook[.]en[.]small-improvements[.]com
- microsoft-outlook[.]en[.]connxusdemo[.]com
- microsoft-outlook[.]en[.]attcorona[.]com
- microsoft-outlook[.]nl[.]slackb[.]com

Sample Malicious String-Connected Subdomains

- microsoftoutlook[.]zip
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com