Dormant Colors IoC Expansion: Don't Install Browser Extensions from These Domains

Table of Contents

Executive Report

Internet users are being tricked into installing browser extensions that can hijack their web searches. The end goal could be to insert affiliate links, but who knows what other malicious activities the threat actors behind them are capable of? To date, cybersecurity researchers have found 30 variants of the extension with more than 1 million combined installs on the Chrome and Edge web stores.

WhoisXML API researchers analyzed the web properties tagged as indicators of compromise (IoCs) in the campaign dubbed "Dormant Colors." Our investigation revealed that:

- 2,400+ domains related to the IoCs through their IP and name server (NS) resolutions, WHOIS records, and text string usage
- A few of the IoCs that still host pages prompting users to download programs and install browser extensions
- Several artifacts connected to the IoCs that host similar types of content

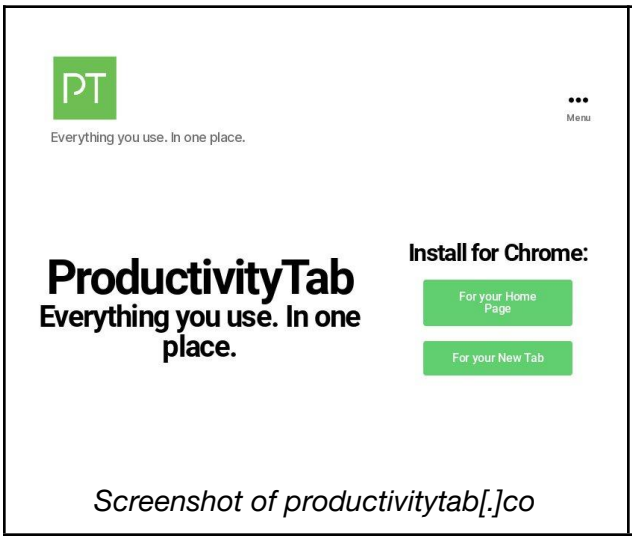
Dormant Colors IoCs through the DNS Lens

Guardio Labs researchers published 34 domains tagged as campaign IoCs. One glance at them tells us that more than half fell under the .xyz space with second-level domains (SLDs) containing 4–6 random alphanumeric characters.

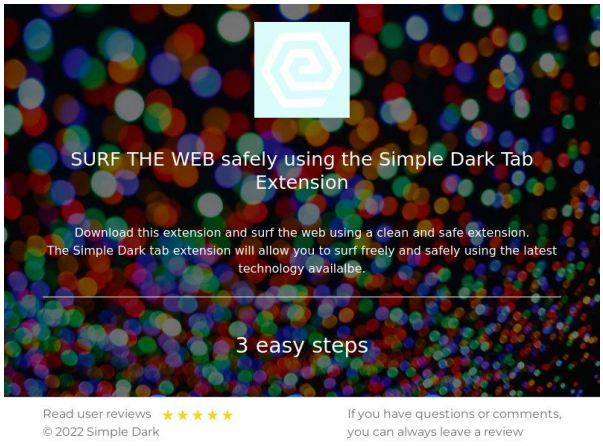
The domains that don't appear to have been randomly generated contained strings like "smash," "offer," and "search."

A bulk WHOIS lookup for the domains revealed four dominant name servers associated with 27 of the IoCs. The registrar of most of the domains was Porkbun, LLC, and all the IoCs had redacted WHOIS records.

As of 31 October 2022, almost all of the IoCs had active IP resolutions. Although most resolved to 404 pages, screenshot lookup results revealed some interesting live content. Below are some examples.



Screenshot of productivitytab[.]co



Screenshot of simpledark-tab[.]com

The content was consistent with that seen from the Dormant Colors campaign, where:

- After being presented with an ad, the target users were asked to download a program or video similar to that offered in productivitytab[.]co.
- Users who attempted to download the app were redirected to another page prompting them to install a color-changing browser extension like that offered by simpledark-tab[.]com.

Finding Artifacts Related to the Dormant Colors IoCs

We used everything we learned from our IoC analysis to look for related web properties with the help of reverse WHOIS and reverse IP/DNS tools. From 34 IoCs, we found 2,428 additional artifacts that we've broken down into the following types.

IP-Connected Artifacts

The active IoCs resolved to more than a hundred IP addresses, most of which were shared or public. We found 7,500+ connected domains, but we narrowed the artifacts down to those that shared the same IP hosts, WHOIS details, and name servers as the domains tagged as IoCs—222 domains fit the bill.

WHOIS-Connected Artifacts

We retrieved all the domains with the .xyz TLD extension and properties starting with the word "smash" added from 1 July to 28 October 2022 that matched the IoCs' WHOIS details. Similarities were seen among them, including:

- The registrar was either Porkbun or Namecheap.
- The registrant organization was either "Private by Design, LLC" or "Privacy service provided by Withheld for Privacy."
- The NSs were terin[.]ns[.]cloudflare[.]com|wanda[.]ns[.]cloudflare[.]com and dan[.]ns[.]cloudflare[.]com|olga[.]ns[.]cloudflare[.]com, exactly the same as those seen in the IoCs' NS WHOIS field.

In sum, we found more than 600 domains connected to the IoCs in the ways described above.

Name Server-Connected Artifacts

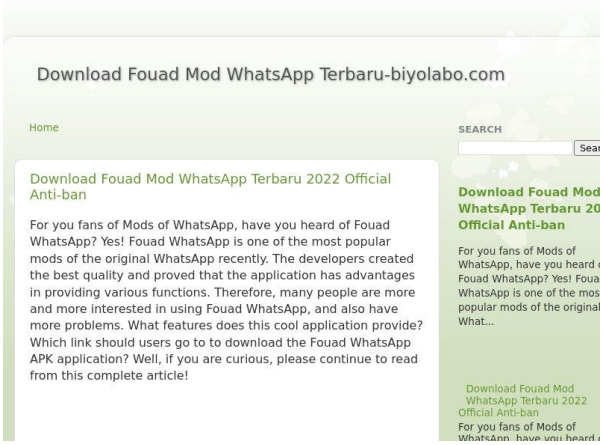
We paid particular attention to the name servers of the domains tagged as IoCs. We found thousands of properties using the four name servers, but narrowed down the list to 1,500+ domains containing the string "search."

Artifact Screenshot Analysis

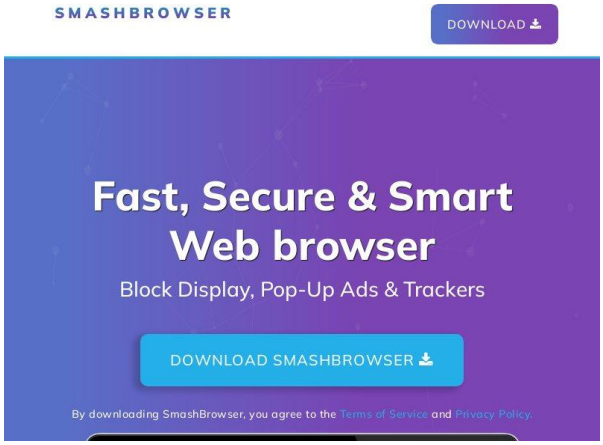
We subjected the connected domains to screenshot lookups and found that several hosted questionable content, including outright phishing pages.

Screenshot of de-sparkasse-tanlegitimation[.]com

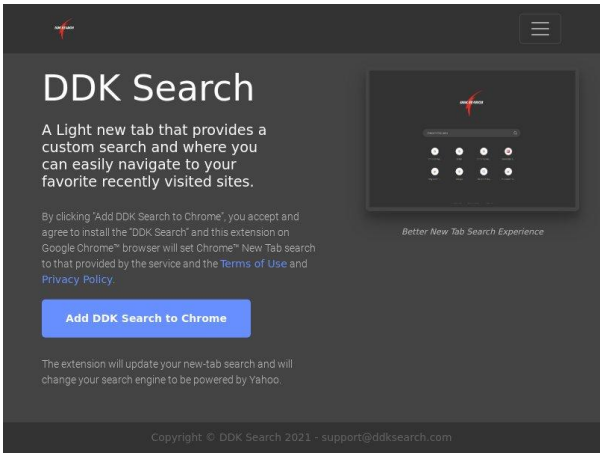
We also detected some domains that hosted content similar to the IoCs that prompted users to download programs and install browser extensions. Below are some examples.



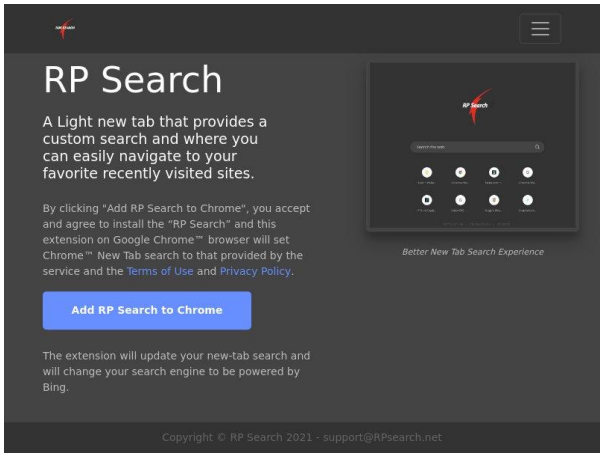
Screenshot of biyolabo[.]com



Screenshot of smashbrowser[.]com



Screenshot of ddksearch[.]com



Screenshot of rpsearch[.]net

—

The Dormant Colors campaign appears to be financially motivated, as its perpetrators aimed to inject affiliate links to hijacked web searches. That may evolve into more malicious and lucrative activities, such as data theft and ransomware infections.

In fact, a bulk malware check on the artifacts revealed several malicious domains, including those that imitated WhatsApp and the decentralized financial platform dYdX. Timely and regular monitoring of digital properties related to IoCs can help mitigate threats.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Domains

Sample IoCs

- isloov[.]com
- changecolorss[.]com
- simpledark-tab[.]com
- toodipex-sucticago[.]icu
- productivitytab[.]co
- smashofferss[.]com
- superofferss[.]com
- smashsearches[.]com
- smashaff[.]com
- 005gs[.]com
- lkbx[.]me
- websearches[.]club
- xcfss[.]xyz
- pelsx[.]xyz
- xcfss3[.]xyz
- eisx2[.]xyz
- lso2[.]xyz
- eisx[.]xyz

- vnhs[.]xyz
- dgopx[.]xyz
- yt5ds[.]xyz
- eisx3[.]xyz
- 666xs[.]xyz
- sikxsx[.]xyz
- bvii[.]xyz
- sokjs[.]xyz
- cs5s[.]xyz
- rssok[.]xyz
- 188xs[.]xyz
- udjx[.]xyz
- zcgxd[.]xyz
- lso1[.]xyz
- eisx4[.]xyz
- xcfss2[.]xyz

Sample Artifacts Related to the IoCs through Their IP Hosts and WHOIS Details

- 02ca1yankee[.]xyz
- 188xs[.]xyz
- 1anizine[.]xyz
- 1cdnlink[.]xyz
- 1wdcv[.]xyz
- 1wios[.]xyz
- 1xslots-12[.]xyz
- 2six[.]xyz
- 326591205[.]xyz
- 366636[.]xyz
- 3doo[.]xyz
- 4ek5eqd7[.]xyz
- 52cjg857[.]xyz
- 5899c[.]xyz
- 598963807[.]xyz
- 5dty[.]xyz
- 5vp5[.]xyz
- 5zkp[.]xyz
- 65945512[.]xyz
- 666aiu[.]xyz
- 711321[.]xyz
- 800014[.]xyz
- 800088[.]xyz
- 8544436[.]xyz
- a51alien[.]xyz
- aaallworkable[.]xyz
- aartedosoutononovastempo[.]xyz
- aatl[.]xyz
- abc[.]huangbuyao1[.]xyz
- adlsena[.]xyz
- ahwroh[.]xyz
- ajmbsghe[.]xyz
- alinemobility[.]xyz
- allfree4gwv[.]xyz
- alphanutrition[.]xyz
- amanbe[.]xyz
- am-anime[.]xyz
- amazingwear[.]xyz
- amkkhot[.]xyz
- anbarsaid[.]xyz
- answer404[.]xyz
- api[.]mrmeomeo[.]xyz
- api[.]spotify[.]gridling[.]xyz
- apicdn13[.]xyz
- apkimp[.]xyz
- appointy[.]xyz
- assortedfair[.]xyz
- australiablob[.]xyz
- autodiscover[.]educatijd[.]xyz
- autoinsurancesum[.]xyz

Sample Artifacts Connected to the IoCs through Their WHOIS Details and Text Strings

- hhyrd1[.]xyz
- vn2jh55[.]xyz
- nmklor[.]xyz
- cggd5[.]xyz
- cxuu66[.]xyz
- tyrw55[.]xyz
- sfg5r[.]xyz
- kd55d[.]xyz
- oooipn[.]xyz
- tuiws5[.]xyz
- jidxx2[.]xyz
- tres69[.]xyz
- v5y8e[.]xyz
- ues5x9[.]xyz
- pyrd5[.]xyz
- mss58r[.]xyz
- nj5sd4s[.]xyz
- ews95[.]xyz
- 5447sg[.]xyz
- iteolkg[.]xyz
- asf69[.]xyz
- xcfss1[.]xyz
- skxj[.]xyz
- eisx4[.]xyz
- lso3[.]xyz
- dgopx[.]xyz
- xcfss3[.]xyz
- eisx3[.]xyz
- eisx[.]xyz
- sokjs[.]xyz
- pelsx[.]xyz
- 188xs[.]xyz
- bvii[.]xyz
- xcfss[.]xyz
- lso1[.]xyz
- lso2[.]xyz
- xcfss2[.]xyz
- 666xs[.]xyz
- cs5s[.]xyz
- eisx2[.]xyz
- smashedpickleball[.]com
- smashbrowser[.]com
- smashtymes[.]com
- smashingfirewall[.]com
- smashtrashtruck[.]com
- smashviber[.]com
- smash-guy[.]com
- smashheroes[.]net
- smashedtater[.]com
- smashbstudio[.]com
- smashacid[.]com
- smashopp[.]com
- smashingspin[.]com
- smashburgerhires[.]com
- smashbeautyhq[.]com
- smashupvip[.]com
- smashberri[.]com
- smashott[.]com
- smash2mining[.]com
- smashinginfo[.]com
- smash-hot[.]com
- smashmirth[.]com
- smashybutton[.]com
- smashpb[.]com
- smashflixtv[.]com
- smashdownburgers[.]com
- smashingsaturday[.]com
- smashstressdown[.]com
- smash-billing[.]com
- smashingsaturdays[.]com
- smashthemandates[.]com
- smashingjade[.]com

- smashedcreations[.]com
- smashingpresence[.]net
- smashingstory[.]com
- smashingplayer[.]vip
- smashprooftext[.]com
- smashedcrabs[.]com
- smashthroughaffiliatemarketingroadblocks[.]com
- smashallergyacademy[.]com
- smashinthebox[.]com
- smashyourmom[.]com
- smashingm[.]com
- smashberlin[.]com
- smashesgiveroses[.]com
- smashversus[.]com
- smashinlabs[.]com
- smashnourishment[.]com
- smashinmatchinfashion[.]com
- smashtrays[.]com
- jekoshop[.]com
- assaultsystems[.]de
- usocci[.]tk
- ndolulapimen[.]tk
- aapu[.]xyz
- bneet[.]net
- raustin[.]com
- chumbru[.]ga
- uress[.]xyz
- coolframes[.]ca
- coolframes[.]com

Sample Properties Flagged as Malicious During the Malware Check Dated 31 October 2022

- australiablob[.]xyz
- chatwhatsaaptante[.]xyz
- dydx-exchangee[.]xyz
- nbay[.]cc
- searchmine[.]net
- jambosearch[.]com
- searches[.]network
- searchdirectsearch[.]net
- searchtipsdiscover[.]com
- find-searchtips[.]net
- searchpersonalized-photo-cards[.]com