Watch Out, That Browser Extension Could Be Cloud9 in Disguise

Table of Contents

Executive Report

Zimperium zLabs threat researchers recently reported the case of the Cloud9 Chrome Botnet, and rightly so. Many of us seem to forget just how much information cybercriminals can steal from our browsers.

Zimperium published seven Cloud9 indicators of compromise (IoCs) to help users protect against the threat. We expanded that list aided by our WHOIS, IP, and DNS tools and found:

- 12 IP addresses to which the IoCs resolved, four of which were malicious
- 443 domains that shared the IoCs' IP hosts
- 1,922 more domains that contained the same strings as the IoCs—"p27rjz4oiu53u4gm," "zmsp," "loginserv," and "cloudminer"
- 12 subdomains that contained the same string combination—"cloud9 + bot"—found among the IoCs
- 10 malicious domains

Blocking the Publicized IoCs May Not Be Enough

Threat actors can't always clean up while and after launching attacks, and the Cloud9 operators, like any other attacker, may have left digital breadcrumbs that we can use to expand the current list of IoCs.

We used the seven domains Zimperium identified as IoCs to jumpstart our investigation. We began by subjecting them to DNS lookups, which led to the discovery of 12 unique IP addresses, six of which are:

- 103[.]198[.]0[.]111
- 107[.]174[.]133[.]119

- 18[.]117[.]28[.]81
- 185[.]184[.]223[.]195
- 202[.]61[.]204[.]169
- 70[.]66[.]139[.]68

Four of these IP hosts—103[.]198[.]0[.]111, 107[.]174[.]133[.]119, 202[.]61[.]204[.]169, and 70[.]66[.]139[.]68—turned out to be malicious. 107[.]174[.]133[.]119 and 70[.]66[.]139[.]68 were, in fact, reported for malicious activity 43 and two times, respectively, on AbuseIPDB. Eight of them pointed to U.S. origins while the remaining four were distributed across Canada, Germany, Japan, and Singapore. Three were hosted by Amazon.com, Inc. and the remaining were spread across six other Internet service providers (ISPs), including Canada-based Shaw Communications, Inc.; Backbone Telecommunications in Singapore; and xTom Limited in Japan.

Next, we used the IP addresses as reverse IP lookup search terms and found 443 more domains. A lot of these seem to also be related to cryptocurrencies in general (e.g., 0ftp[.]crypto-webminer[.]com, auth[.]crypto-webminer[.]com, and upload[.]crypto-webminer[.]com) and specific coins (e.g., bitcoin-pocket[.]eu, 00kemya00[.]anikapedia[.]bnbcraft[.]com, and 0moneroocean[.]crypto-webminer[.]com).

Using this list of cryptocurrencies as reference, we looked at how many domains contained "crypto" and some coins' names.

Domain names suggesting they're sources of generic crypto web miners dominated, followed closely by Bitcoin-themed domains. It isn't surprising to see more "bitcoin"-containing domain names, given that the cryptocurrency still commands the highest monetary equivalent.

We also identified unique strings used among the IoCs, specifically "p27rjz4oiu53u4gm," "zmsp," "loginserv," and "cloudminer." Domains & Subdomains Discovery domain searches for these strings allowed us to uncover 1,922 additional web properties. Ten of the total 2,365 domains turned out to be malicious. We listed five of them below.

- cloudminers[.]us
- loginservice[.]gq
- cloud-loginserv[.]top
- loginserverfrengki[.]cf
- myinboxloginservice[.]com

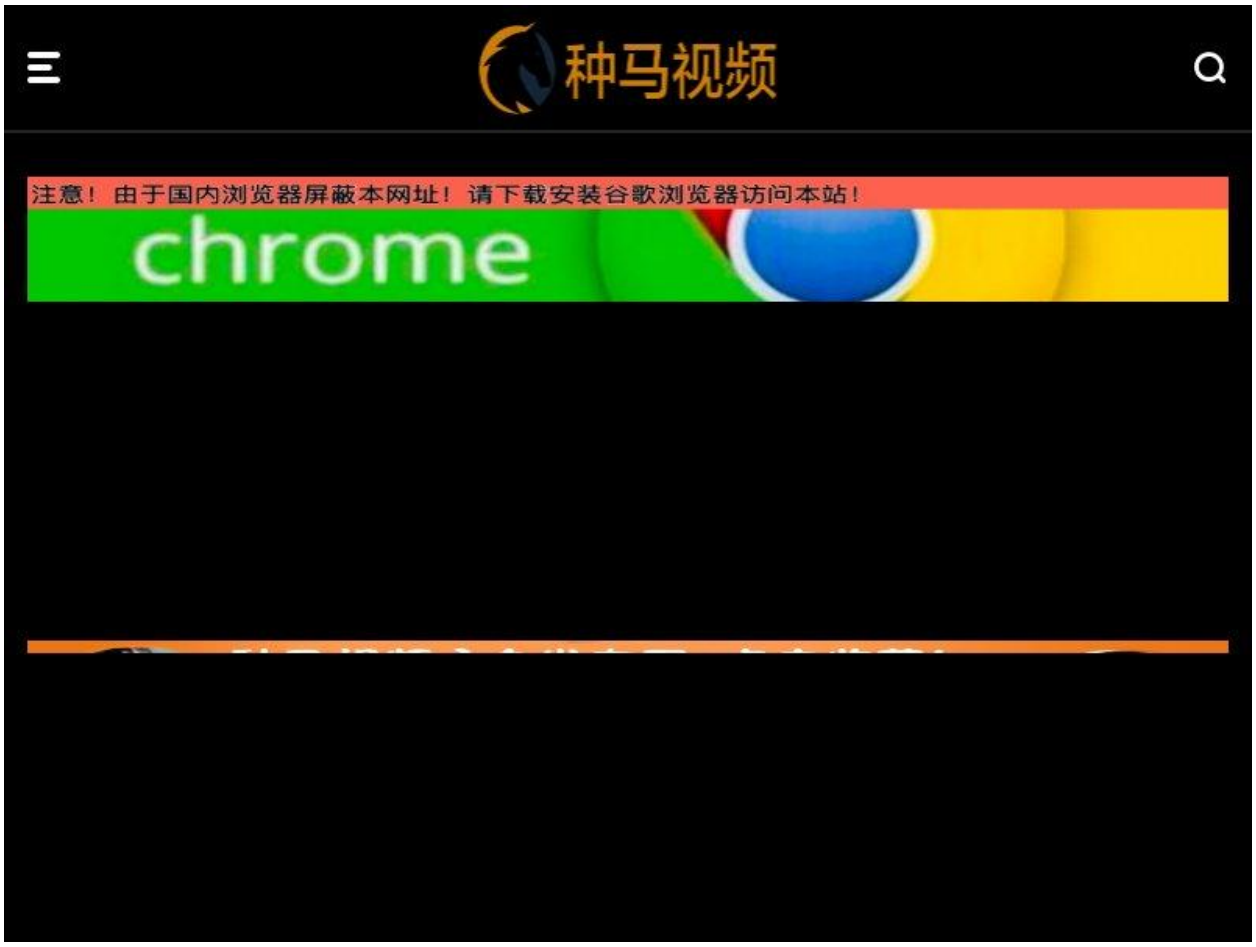
One of the malicious domains—ezmspcloud[.]com—was a confirmed spam sender while the remaining nine were malware hosts.

Apart from the malicious domains above, adding the following to monitoring lists may also be worth it given that they contain the names or brands of legitimate companies despite not belonging to them based on WHOIS record comparisons:

- wecloudminers[.]com (WeCloud)
- dogecloudminer[.]co (Dogeminer)
- cloudminerbtc[.]com (Bitcoin)
- oraclecloudminer[.]com (Oracle)
- googleloginservice[.]tk (Google)
- facebookloginserver[.]tk (Facebook)
- icloud-loginservice[.]com (iCloud)
- appleweibloginserver[.]com (Apple)
- paypal-loginservice[.]com (PayPal)
- alibabaloginservice[.]com (Alibaba)

Any of these additional domains could also figure in phishing campaigns targeting the companies whose names or brands appear in them.

Screenshot lookups for the 2,000+ domains yielded interesting results as well. The domains below, for instance, sported the Chrome logo even if it doesn't belong to Google as per a WHOIS record comparison.



Screenshot of 810hao[.]com

We also looked for subdomains containing the same string combination—"cloud9 + bot"—as some of the IoCs. That led to the discovery of 12 subdomains. While none of them were malicious, a majority of them could be connected to the malicious Cloud9 infrastructure, including these five:

- botpress[.]cloud9[.]mattsgreen[.]net
- discordbot[.]cloud9c[.]repl[.]co
- discord-bot-1[.]cloud9c[.]repl[.]co
- forge-trybot[.]gamma[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]dev-akulb[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev

—

Our IoC expansion exercise allowed us to identify four additional malicious IP addresses and 10 malicious domains that are or could be connected to Cloud9. Users would do well to avoid accessing them. Network administrators, meanwhile, may want to include them in their blocklists for utmost threat protection.

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 Artifacts and IoCs

Sample Domains That Shared the IoCs' IP Hosts

- 0-0-0-0[.]xyz
- 0-0-8[.]com
- 0-111[.]com
- 0-ads-free-web-page-hosting[.]buzz
- 0-carbon[.]net
- 0-carbon[.]org
- 0[.]credit
- 0[.]easyhash[.]de
- 00-54[.]com
- 00-jlbond[.]iqbc[.]net
- aaumndtzitjo25l77z2sehj64zryae2d6dqoqv5qnpoiyaaehz5cs2ad[.]onion[.]link
- achocolatado[.]com
- akaphil[.]com
- animalarts[.]com[.]br
- annj6xiap5pfuejt[.]tor2web[.]org
- aoqtq[.]com
- ar-ar[.]facebookcorewwwi[.]onion[.]link
- auth[.]crypto-webminer[.]com
- avastvpn[.]com
- babys465y2piyqqa6hrwwqjhja43htztqgx6jaxleuxxuqb7soflfwid[.]onion[.]link
- bcled[.]net
- bitcoin-cashcard[.]com
- bitcoin-cashcard[.]de
- bitcoin-pocket[.]eu
- bjbaof[.]com
- broskymedia[.]org
- cavetord6bosm3sl[.]onion[.]link
- ce5sbcv5b75jvur4[.]tor2web[.]org
- chianmarket[.]com
- cmacc[.]org
- cqyami[.]com
- ctroneum[.]crypto-webminer[.]com
- dashanjiao[.]com
- de6ygxmb3m3pxosh[.]onion[.]link
- dg7c4ams7iocjpou[.]onion[.]link
- dh5vymzcmjy6lmew7e2iz3bcirjfxgav3dn6t2tnxauoohqe5tdviiid[.]onion[.]link
- dhcjn[.]com
- disney6dvzs62ckd2pcpageusw2je3m24ubk6qn2bq26dti5absp6yqd[.]onion[.]link
- dontbeevils[.]de
- dream-guide[.]com
- easyhash[.]de
- edown[.]org
- esseafro[.]com

- eth-pocket[.]de
- evilsbedont[.]de
- father-and-teen[.]pedolnksijylohjrzykfc3fmi6e3fuyxngtxxaz2urmbznb7jcdovcyd[.]onion[.]link
- freeipdb[.]org
- gcgbz[.]com
- golider[.]com
- gs7mpabfzdsqwei7vvcr27aw7gzq7ynkjzqwv23gvtc5dcpiououn4qd[.]onion[.]link

Sample Domains That Shared Strings Found among the IoCs

- 0fficecloud-loginserv[.]com
- 1cloudminers[.]com
- 1wzmsp[.]top
- 2019zwzmsp[.]info
- 247cloudminer[.]com
- 2cloudminers[.]com
- 2seizmsph-u2x[.]click
- 2zmspm[.]cyou
- 34zmsp[.]cn
- 3ug-zmsppi3k[.]tk
- a2zmsp[.]com
- accessloginservices[.]com
- accinfologinservices[.]co[.]uk
- accinfosloginservices[.]co[.]uk
- accloginservice[.]cf
- account-failed-loginservice[.]com
- account-loginserv[.]com
- account-loginservices[.]com
- accountfailedpaymentloginservice[.]com
- accountinfologinservices[.]co[.]uk
- bankierensesamloginservlet[.]ru
- bardlogloginservieserver[.]com
- bardlogloginservieserver[.]net
- bardlogloginservieserver[.]org
- bcloudminer[.]com
- bestbizmsp[.]com
- bestcloudminer[.]info
- bestcloudminers[.]com
- bfnmzmspy[.]com
- bgpkzmsp[.]science
- cbzmsp[.]com
- cch-cloudminer[.]com
- cchcloudminer[.]com
- cchcloudminer[.]ga
- cchcloudminer[.]link
- cchcloudminer[.]net
- cchcloudminerreview[.]com
- cczmspa[.]com
- chezmsphone[.]com
- chiacloudminer[.]com
- d8zmspp[.]ga
- datacloudminer[.]com
- datasecureaccountloginserveirc[.]com
- dbzmspjz9l0uzktxn7[.]ph
- ddzmspfn[.]loan
- de-loginservice-toaccount[.]com
- dgszmsp[.]com
- dgzmsp[.]com
- dhdtz2ovebzmsp4k46[.]link
- dhzmsplc[.]loan
- e3hzmsp[.]top
- ecloudminer[.]com
- egedenizotizmspor[.]com
- egedenizotizmspor[.]net
- egedenizotizmspor[.]org
- ejqzmsp[.]ga

- eldersafeloginserver[.]com
- elitecloudminers[.]com
- eloginserver[.]net
- elvbzmsp[.]ml
- facebookloginserver[.]tk
- facebookloginservice[.]com
- fantazmsports[.]com
- fbloginserver[.]com
- fbloginservice[.]com
- fbloginservicemanager[.]site
- fbs-loginserv[.]cf
- fgzmsp[.]co
- fhzmsp[.]loan
- fitizmsports[.]com
- g9pzmsp[.]us
- gaezmsps[.]men
- gateloginservice[.]xyz
- gazellezmsp[.]com
- gcloudminers[.]com
- genesiscloudminer[.]com
- gf5zmsphe6-nk[.]biz
- gistkwfk0v0upntw0yv4bqewj6f7azmsp6erxkee2gcbgqfu[.]ws
- gkzmsp[.]fun
- gkzmsp[.]icu
- h6tzmsp4p[.]com
- hashcloudminer[.]com
- hashcloudminer[.]net
- hashcloudminer[.]online
- hashcloudminers[.]co
- hashcloudminers[.]com
- hazmsp[.]co[.]uk
- hdhplzczmspzzxz[.]nom[.]za
- heritagecloudminers[.]com
- hfszmspa[.]com
- icczmsp[.]biz
- icfzmspe[.]tk
- icloud-loginservice[.]com
- icloudminer[.]com
- icloudminers[.]com
- id-loginservices[.]com
- ilzmspogxz[.]biz
- ilzmspuv[.]space
- inaemrick2zmsp02[.]cf
- incloudminers[.]com

Subdomains That Shared a String Combination Found among Some of the IoCs

- cloud9robotics[.]monartnational[.]us
- botpress[.]cloud9[.]mattsgreen[.]net
- discordbot[.]cloud9c[.]repl[.]co
- www[.]cloud9robotics[.]monartnational[.]us
- discord-bot-1[.]cloud9c[.]repl[.]co
- cloud9robotics-com[.]mail[.]protection[.]outlook[.]com
- forge-trybot[.]prod[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]alpha[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]gamma[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]dev-akulb[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]dev-yuxnl[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev
- forge-trybot[.]dev-scalmich[.]infrastructure[.]silk[.]cloud9[.]aws[.]dev