Catching Batloader Disguised as Legit Tools through Threat Vector Identification

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

Putting on a mask on malware has always worked to trick users into downloading them, and the threat actors behind Batloader banked on just that. Trend Micro researchers tracked and analyzed Batloader-related developments toward the end of 2022. They identified 17 domains as indicators of compromise (IoCs) (see the table below), including three that rode on the popularity of Black Friday offers—a well-known cybercriminal tactic to lure users to download malware.

Batloader IoCs	
• zoomofferblackfriday[.]com • updatecloudservice1[.]com • updateclientssoftware[.]com • updatea1[.]com • t1pixel[.]com • slackcloudservices[.]com • logmeinofferblackfriday[.]com • internalchecksso[.]com • installationupgrade6[.]com	• installationsoftware1[.]com • grammarlycheck2[.]com • externalchecksso[.]com • cloudupdatesss[.]com • clodtechnology[.]com • anydeskofferblackfriday[.]com • 24xpixeladvertising[.]com • 105105105015[.]com

WhoisXML API researchers worked on adding the following artifacts to the existing list:

- Two unredacted registrant email addresses that led to the discovery of an additional malicious domain
- Five IoC IP resolutions, two of which turned out to be malicious
- 318 domains that shared the IoCs' IP hosts, 35 of which have been confirmed to be malware hosts

- 2,283 domains that contained strings found among the IoCs, 69 of which have been dubbed malicious
- 2,875 domains that contained the names of the companies Batloader targeted
- 1,158 of the 2,875 domains with the target brand names had unredacted ownership details, 51 of which were confirmed malware hosts

Identifying Potential Threat Vectors through WHOIS Connections

A bulk WHOIS lookup for the IoCs led to the discovery of two unredacted email addresses used to register two of the domains.

Reverse WHOIS searches for these artifacts allowed us to identify a yet-unpublicized domain—***t1pixelsite[.]com***—that turned out to be malicious, too. What's more interesting, though, is that this artifact contained the string ***t1pixel*** akin to the IoC ***t1pixel[.]com***, including the same TLD extension, apart from having the same registrant. A comparison of the two domains' WHOIS records showed similarities in their registrar (PDR Ltd.) and creation date (9 November 2022).

These findings could indicate that ***t1pixelsite[.]com*** is part of the Batloader infrastructure and should be blocked as well.

Uncovering More Artifacts through DNS Relations

Next, we sought to find more digital breadcrumbs through the DNS lens.

DNS lookups for the IoCs showed they resolved to five IP addresses that don't appear in the Batloader report. Two of these were confirmed to be malware hosts and may warrant blocking on users' part—***194[.]67[.]110[.]215*** and ***194[.]67[.]119[.]190***.

To find more potential threat entry points, we subjected the IP addresses to reverse IP/DNS lookups that enabled us to collate 318 domains. A bulk malware check for these artifacts showed that 35 were malicious. Blocking access may be critical as they, like the IoCs, could be serving Batloader.

Since the IoCs contained identifiable unique strings (see the table below for the list), we then sought to find more domains that shared them.

Domains & Subdomains Discovery Search Strings Used	
• ***zoomofferblackfriday.***	• ***installationsoftware*.***

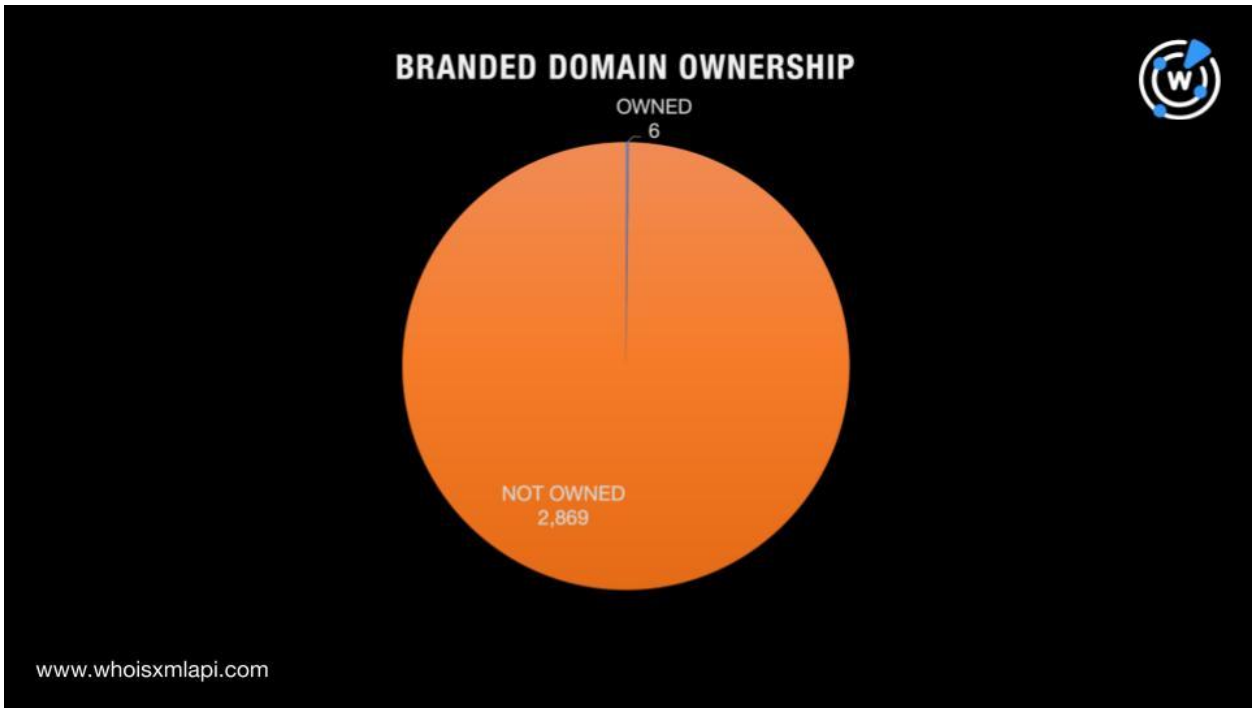
• ***updatecloudservice*.*** • ***updateclientssoftware.*** • ***updatea*.*** • ***t1pixel.*** • ***slackcloudservices.*** • ***logmeinofferblackfriday.*** • ***internalchecksssso.*** • ***installationupgrade*.***	• ***grammarlycheck*.*** • ***externalchecksso.*** • ***cloudupdatesss.*** • ***clodtechnology.*** • ***anydeskofferblackfriday.*** • ***24xpixeladvertising.*** • ***105105105015.***

Our Domains & Subdomains Discovery searches found 2,283 more artifacts, 69 of which have been dubbed malware hosts. All of them contained the string ***update***.

Unveiling Typosquatting Properties through Domain Discovery

Trend Micro's Batloader analysis listed 25 legitimate tools the malware posed as. We used these brands to seek out other potential attack vectors, specifically domains, created just last month.

Out of these 25 organizations, only 13 had unredacted WHOIS records—Adobe, CCleaner, FileZilla, Fortinet, GetNotes, Java, LogMeIn, Putty, Schwab, Slack, TradingView, Zoho, and Zoom. Based on this list, we performed record comparisons for the 2,875 domains possibly mimicking these companies. Of these, only six were actually owned by the companies the threat actors mimicked.



The table below shows the branded domain ownership breakdown.

Branded Domain Ownership Shares		
Target Company	**Owned**	**Not Owned**
Adobe	1	231
CCleaner	0	32
FileZilla	0	10
Fortinet	0	13
GetNotes	0	2
Java	0	930
LogmeIn	0	2
Putty	0	16
Schwab	0	102
Slack	0	157
TradingView	0	130
Zoho	5	86
Zoom	0	1,158

A bulk malware check for the domains containing the brands mentioned in the Batloader report showed that 51 of them were malicious.

—

Our IoC list expansion uncovered 5,484 web properties that could be part of the Batloader infrastructure. Of these artifacts, 158 turned out to be malicious and warrant blocklist addition. In addition, the organizations Trend Micro dubbed as Batloader imitation targets may wish to report 1,100+ domains that contained their brands as domain strings for typosquatting as part of their brand protection efforts.

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 IP Addresses to Which the IoCs Resolved

- 31[.]31[.]199[.]253
- 194[.]67[.]92[.]245
- 172[.]105[.]103[.]207

Sample Domains That Shared the IoCs' IP Hosts

- 194-67-110-215[.]cloudvps[.]regruhosting[.]ru
- 194-67-119-190[.]cloudvps[.]regruhosting[.]ru
- 194-67-92-245[.]cloudvps[.]regruhosting[.]ru
- 2mblk[.]com
- 31-31-199-253[.]cloudvps[.]regruhosting[.]ru
- 43nutrientes[.]com
- 4g796aiv4kj1[.]world
- 5pneuovxi22i4fagh9[.]today
- 7-eleven-handbags[.]com
- 8tril[.]com
- a-plague-tale[.]top
- abrakadabras[.]net
- abvtqhwodwjmi[.]work
- accemfsqovkd[.]pw
- account[.]adfs[.]kyivstar[.]online
- acerthk3v9fvsby5n[.]today
- acjhwpdjhlhbncf[.]click
- acronicssolutions[.]org
- adams679[.]drcopps[.]com
- adams879[.]pelangiqq99[.]com
- adfs[.]kyivstar[.]online
- admiral-juegos[.]com
- adobe-update[.]net
- adobestats[.]com
- adsdsadsalifsa[.]digital
- agceram[.]com
- aliensdrop[.]com
- allen1037[.]pelangiqq99[.]com
- allen139[.]drcopps[.]com
- allen618[.]drcopps[.]com
- allow-access[.]com
- allsofttech[.]com
- amakeperfeita[.]online
- ampjsppmftmfdblpt[.]info
- anderson360[.]pelangiqq99[.]com
- anderson576[.]pelangiqq99[.]com
- anderson856[.]drcopps[.]com
- anderson858[.]drcopps[.]com
- antichltabompadre[.]com
- anz1guftr2hdaqq3w[.]agency
- asdakasma[.]digital
- asiaworldremit[.]com
- autoconfig[.]celikklczet[.]com
- autoconfig[.]simsekaluminyurn[.]com
- autodiscover[.]celikklczet[.]com
- autodiscover[.]simsekaluminyurn[.]com
- autofileupdater[.]com
- avasecurityservices[.]com
- bamya9[.]com
- bdappbk[.]imperialmm[.]com

Sample Malicious IP-Connected Domains

- 194-67-119-190[.]cloudvps[.]regruhosting[.]ru
- 2mblk[.]com
- 5pneuovxi22i4fagh9[.]today
- 7-eleven-handbags[.]com
- a-plague-tale[.]top
- ampjsppmftmfdblpt[.]info
- boxkron[.]com
- challenge-identifier[.]com
- cinetfox[.]com
- devciscoprograms[.]com
- dmvb4e5ypx75[.]world
- echoesdesing[.]com
- googleanalyticstag[.]com
- greekrestaurantgustosa[.]com
- hpronto[.]settings[.]carnegieinsider[.]com
- identamazononline[.]com
- imperialmm[.]com
- liveme1[.]com
- lluxll[.]digital
- login[.]adfs[.]kyivstar[.]online

Sample Domains That Contained Strings Found among the IoCs

- updatecloudservice[.]com
- updateacts[.]com
- updateantelope[.]com
- updateaccc[.]co
- updateandverification[.]com
- updateappserver[.]com
- updateaccptmdw3[.]com
- updateagentwebsite[.]com
- updateanjay2[.]com
- updateappmail[.]com
- updateamazonacountmail[.]xyz
- updateamazonacount[.]buzz
- updateauth[.]gq
- updateappleid-com[.]tk
- updateaccount-limitedaccess-signin-information[.]ga
- updateau[.]cc
- updateab5[.]org
- updateassurance[.]com
- updatealexa[.]website
- updateactivation[.]review
- updateapproved[.]services
- updateadovesettings[.]io
- updateaccount-information[.]co[.]uk
- updateauto[.]tech
- updateandrenovate[.]net
- updateappaccountidinformation[.]org
- updateadata[.]store
- updateaccsesid[.]com
- updateappmobilos[.]com
- updateaccount[.]asia
- updateacc[.]net
- updateappliduppaccserverirc[.]com
- updatearena[.]ml
- updateallsafe[.]bid
- updateaccount-paypasecure[.]com
- updateautosafe4allos[.]online
- updateadobeflash[.]gq
- updateautosysformacandpc[.]info
- updateavailability[.]com
- updateadviser[.]com
- updateaccountinformations[.]com
- updateapkreviews[.]com
- updateadvancedcompletelyprogram[.]icu
- updateadvancedextremelyproduct[.]icu
- updateaccount-verif[.]com
- updatealert[.]club
- updatealert[.]website
- updateamazon-co-jp[.]com
- updateamazon-service[.]com

- updateaccountssecurity[.]org
- updateaccountpen09[.]com
- updatealibaba[.]cpa
- updateaccountunsual2019-paypal[.]com
- updateaccount[.]tk
- updateautosafe4newsystems[.]online
- updateaddress-ups[.]com
- updateaccount-intl[.]com
- updateappssnyc001[.]net
- updateappsdownloads[.]com
- updatealert09x-info[.]gq
- updateaccsecure-paymentcare[.]org
- updateall-emailstorage[.]tk
- updateauthwfargo[.]tk
- updateaccountid[.]ga
- updateaccount-information[.]com
- updateadata[.]org
- updateacinfo[.]cf
- updateaccounts-ksaa[.]online
- updateally[.]online
- updateaccount-new[.]online
- updateactualinotiglcuenta[.]xyz
- updateaddressnow[.]org
- updateaccountseoops[.]gq
- updateaktifbank[.]ph
- updateaero[.]co
- updateadvertising[.]com
- updatea-appleid[.]com
- updateaccbilling[.]co[.]uk
- updateac[.]xyz
- updateamazonpluscard[.]monster
- updateamazonpluscard[.]xyz
- updateacountrakutenmail[.]top
- updateamazonacount[.]xyz
- updateadd[.]fr
- updateagreements[.]com
- updateal[.]com
- updateafex[.]fm
- updateall[.]com
- updateanalytics[.]net
- updateaccountdetails[.]com
- updateairline[.]com
- updateabc[.]com
- updateadv[.]ro
- updateanalytics[.]com
- updateandrenovate[.]com
- updateapp[.]com
- updateaccs[.]us
- updateantivir[.]us
- updateatomygov[.]top
- updateaceh[.]com

Sample Malicious String-Connected Domains

- updatecloudservice[.]com
- updateactivation[.]review
- updateadovesettings[.]io
- updateautosafe4allos[.]online
- updateaddress-ups[.]com
- updatealert09x-info[.]gq
- updateaccsecure-paymentcare[.]org
- updateall-emailstorage[.]tk
- updateamazonacount[.]xyz
- updateable[.]info
- updateaccountslimit[.]com
- updateaccount-information-center2652164546672367 56recovery[.]com
- updateaccountapplesupport-63g1[.]com
- updateapps-aacounts[.]ga
- updateavenue1[.]com
- updateaccountinformationaccess[.]net
- updateas-co-jp-comcenter[.]xyz
- updatea[.]xyz
- updateaccountinfomation[.]com

- updatealert[.]support

Sample Domains That Contained the Brands Mentioned in the Batloader Analysis

- xn--obe-8oa4e[.]vg
- iradobe[.]ir
- adobe-fa[.]ir
- adobes[.]blog
- adobe-cs[.]cn
- adobepp[.]com
- getadobe[.]co
- adobeai[.]art
- kadobet[.]art
- adobesho[.]ir
- topadobe[.]ru
- adobe[.]org[.]tr
- aadobe[.]space
- casadobel[.]de
- gptadobe[.]com
- adobeb2b[.]com
- wv-adobe[.]top
- hadobey[.]life
- adobeposa[.]vg
- adobefood[.]cn
- adobes7[.]blog
- mhsadobe[.]org
- adobegpt[.]com
- kadobedim[.]ir
- ob1adobe[.]com
- adobe-apps[.]us
- luxeadobe[.]com
- adobehalt[.]top
- horadobet[.]net
- vwv-adobe[.]top
- vvw-adobe[.]top
- adobeppro[.]com
- withadobe[.]win
- horadobet[.]com
- sabadobet[.]com
- adobe-com[.]top
- madobeniot[.]ir
- fameadobe[.]top
- adobeeflsh[.]vg
- radobest[.]site
- all4adobe[.]com
- weadobe[.]co[.]za
- www-adobe[.]xyz
- adobefail[.]com
- adobe-csc[.]com
- ind-adobe[.]com
- horadobet[.]org
- adobelamb[.]top
- hahnadobe[.]top
- tornadobet[.]xyz
- adobeaadjei[.]co
- adobeceres[.]top
- adobetut01[.]top
- adobero[.]beauty
- sabadobet[.]site
- horadobets[.]com
- madobesan[.]arab
- tornadobelt[.]ir
- ilhadobeca[.]com
- adobe[.]tokyo[.]jp
- horadobet[.]club
- ubladobein[.]xyz
- adobethelaw[.]co
- 225adoberd[.]com
- winteradobe[.]it
- adobeincopy[.]vg
- bravadobear[.]com
- winteradobe[.]com
- adobeorders[.]com
- supportadobe[.]vg

- screenadobe[.]com
- adobe-apps[.]site
- adobeexpress[.]us
- tornadobet[.]mobi
- topadobe[.]online
- adobetuition[.]vg
- adobebiotic[.]top
- adobestopck[.]com
- www-adobeus[.]top
- mostlyadobe[.]com
- rtpkadobet[.]info
- adobemailva[.]pro
- expressadobe[.]us
- adobe3to5[.]online
- cambriadobes[.]org
- adobeappdesk[.]com
- adobeexpress[.]top
- adobeteacher[.]com
- adobecontent[.]com
- adobekern[.]online
- adobeflashsj[.]com
- horadobet[.]online
- adobepro[.]express
- adobeague[.]online
- adobecreekrp[.]com
- adobe-cloud[.]shop
- expressadobe[.]top
- adoberanchms[.]com
- podcastadobe[.]com
- adobecommerce[.]se

Sample Malicious Brand-Connected Domains

- wv-adobe[.]top
- adobe-com[.]top
- adobelamb[.]top
- adobeappdesk[.]com
- www-adobe-com[.]top
- adobe-documents[.]gq
- adobe-photoshop[.]top
- adobepresetforyou[.]us
- www-fortinet-com[.]top
- javaadroit[.]top
- now-javaburn[.]store
- softputty[.]com
- putty-app[.]com
- wvvslack[.]top
- wvwslack[.]top
- slack-com[.]top
- wvw-slack[.]top
- slacknow[.]tech
- slackapp[.]tech
- slackapp[.]store