脅威ベクトルの特定で正規のツールを偽るBatloaderを発見

目次

要旨

ユーザーを騙してマルウェアをダウンロードさせるため、脅威アクターはしばしばマルウェアに仮面をかぶせます。Batloaderの背後にいた攻撃者もその手法を使いました。トレンドマイクロの研究者は、2022年末にかけてBatloader関連の動向を追跡・分析し、17個のドメイン名をIoC（セキュリティ侵害インジケーター）として特定しました（下表）。そのうち3つのドメイン名は、ブラックフライデーのセールに便乗したものでした。これは、マルウェアをダウンロードさせるサイバー犯罪の手口としてよく知られたものです。

Batloader関連のIoC	
• 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では、上記のIoCリストを拡充する調査を行いました。その結果、連鎖的に以下を発見しました。

- ドメイン名登録者の未編集のメールアドレス2つ。それらから悪意あるドメイン名をさらに特定
- IoCとされたIPアドレスが解決したドメイン名5つ。そのうち2つは悪意あるドメイン名であると確認
- IoCと同じIPアドレスを使っている318個のドメイン名。そのうち35個はマルウェアホストであると確認

- IoCで使われているものと同じ文字列を含む2,283個のドメイン名。そのうち69個は悪意あるドメイン名と確認
- Batloaderが標的にした企業の名称を含む2,875個のドメイン名。
- 標的の名称を含む2,875個のドメイン名のうち1,158個については、登録者の情報が未編集で公開。そのうち51個はマルウェアホストと確認

WHOISデータの関連性から潜在的脅威ベクトルを特定

上記のIoCをbulk WHOIS lookupで検索したところ、2つのドメイン名の登録に使われた未編集のメールアドレスが2つ見つかりました。

それらをReverse WHOIS searchesでさらに調べた結果、まだ公開されていないドメイン名***t1pixelsite[.]com***を特定でき、それも悪意あるドメイン名であるとわかりました。興味深いことに、この***t1pixelsite[.]com***はIoCである***t1pixel[.]com***と共通の登録者によって取得されたドメイン名でした。また、IoCの***t1pixel[.]com***と同様に***t1pixel***という文字列を含んでおり、TLDも***t1pixel[.]com***と同じ.comです。この2つのドメイン名のWHOISレコードを比較したところ、レジストラ（PDR Ltd.）とレコード作成日（2022年11月9日）が同じでした。

こうした結果は、***t1pixelsite[.]com***がBatloaderのインフラの一部であること、既知のIoCと同様にブロックされるべきドメイン名であることを示唆しています。

DNSの関連性からさらにアーティファクトを発見

次に、IoCのドメイン名をDNS lookupsにかけたところ、Batloaderのレポートにはない5つのIPアドレスに名前解決しました。そのうち2つ（***194[.]67[.]110[.]215*** と ***194[.]67[.]119[.]190***）はマルウェアのホストであることが確認されており、ユーザー側でブロックする必要がありそうです。

潜在的な脅威のエントリポイントをさらに見つけるため、上記のIPアドレスをreverse IP/DNS lookupsで検索してみました。その結果、318名のドメイン名を特定できました。これらを一括してマルウェアチェックしたところ、35件が悪意あるドメイン名と判明しました。IoCと同様にBatloaderを提供している可能性があり、アクセスをブロックするべきかもしれません。

IoCには固有の文字列が含まれていたため、同じ文字列を含むドメイン名をさらに探しました。

Domains & Subdomains Discovery で使用した検索ワード	
• ***zoomofferblackfriday.***	• ***installationsoftware*.***

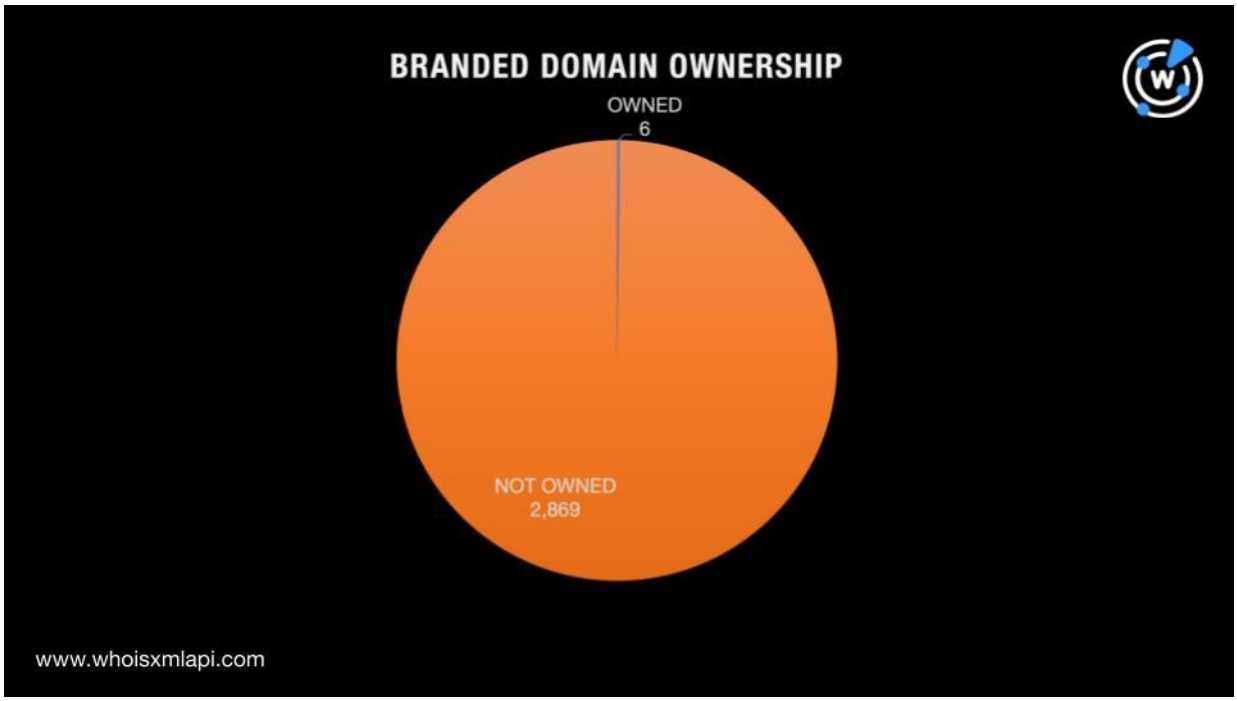
• ***updatecloudservice*.*** • ***updateclientssoftware.*** • ***updatea*.*** • ***t1pixel.*** • ***slackcloudservices.*** • ***logmeinofferblackfriday.*** • ***internalchecksso.*** • ***installationupgrade*.***	• ***grammarlycheck*.*** • ***externalchecksso.*** • ***cloudupdatesss.*** • ***clodtechnology.***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

当社のDomains & Subdomains Discoveryで検索した結果、2,283個のドメイン名を特定できました。そのうち69個はマルウェアホストでした。そして、全てのドメイン名が***update***という文字列を含んでいました。

Domain Discoveryでタイポスクワッティングのドメイン名を特定

トレンドマイクロのBatloaderの分析では、このマルウェアが偽装した25の正規のツールをリストアップしています。当社は、それらのツールのブランド名をもとに、2023年1月に作成されたばかりの他の潜在的な攻撃ベクトル、特にドメイン名を探し出しました。

25のツールを提供している組織のうち、WHOISレコードが非公開になっていないのは13組織（Adobe、CCleaner、FileZilla、Fortinet、GetNotes、Java、LogMeIn、Putty、Schwab、Slack、TradingView、Zoho、Zoom）でした。その13の組織を擬装していると思われる2,875個のドメイン名についてWHOISレコードを比較したところ、正規の組織が実際に所有していたドメイン名はわずか6つであることがわかりました。



各ブランドのドメイン名所有者の内訳は、以下の通りです。

ブランドドメイン名の所有者の内訳		
標的にされた企業	**その企業が所有する ドメイン名**	**その企業の所有でない ドメイン名**
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

Batloaderのレポートに記載されていたブランド名を含むドメイン名を一括してマルウェアチェックしたところ、51件が悪意あるドメイン名と確認されました。

—

IoCリストをもとに展開した当社の調査により、Batloaderインフラの一部となり得る5,484個のウェブプロパティが新たに発見されました。このうち158個は悪意があるため、ブロックリストへの追加が必要です。また、トレンドマイクロのレポートでBatloaderの標的として言及された組織は、自社ブランドを文字列として含む1,100個あまりのドメイン名をタイポスクワッティングとして通報することが望ましいでしょう。

同様の調査をご希望のお客様、またはこの調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合せください。

付録：アーティファクトとIoCの例

IoCが名前解決したIPアドレスの例

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

IoCと同じIPアドレスを使用していたドメイン名の例

- 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

共通のIPアドレスを使用していた悪意あるドメイン名の例

- 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

IoCと共通の文字列を含むドメイン名の例

- 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

共通の文字列を含む悪意あるドメイン名の例

- 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-center26521645466723675 6recovery[.]com
- updateaccountapplesupport-63g1[.]com
- updateapps-aacounts[.]ga
- updateavenue1[.]com
- updateaccountinformationaccess[.]net
- updateas-co-jp-comcenter[.]xyz
- updatea[.]xyz
- updateaccountinfomation[.]com

- updatealert[.]support

Batloaderの分析で言及されたブランド名を含むドメイン名の例

- 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

共通のブランド名を含む悪意あるドメイン名の例

- 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