How the SVB and Credit Suisse Crash Was Reflected in the DNS

Table of Contents

Executive Report

We've proven time and again that the effects of current events always extend to the DNS. Just last month, two big banks—the Silicon Valley Bank (SVB) and Credit Suisse—collapsed. Financial experts said more banks may be bound to follow.

WhoisXML API sought to discover how the closure of the two banks and similar recent events are reflected in the DNS. We specifically looked into the cases of SVB, Credit Suisse, Silvergate Capital Corp., Signature Bank, and the First Republic Bank. All of these institutions faced great turmoil just days in-between in March of this year. Our foray into the DNS revealed:

- 1,220 domains containing the strings ***siliconvalleybank***, ***creditsuisse***, ***silvergatecapital***, ***signaturebank***, and ***firstrepublicbank***, 20 of which turned out to be malicious
- 3,902 subdomains containing the strings ***siliconvalleybank***, ***creditsuisse***, ***silvergatecapital***, ***signaturebank***, and ***firstrepublicbank***, three of which turned out to be malware hosts
- 31 domains and one subdomain containing the string ***bankcollapse***
- 278 domains and 420 subdomains containing the string ***bankalert***, 21 and 12 of which, respectively, turned out to be malicious
- 124 domains and 197 subdomains containing the string ***bankupdate***, eight and 23 of which, respectively, turned out to be malware hosts

Gauging the Effects of Bank Collapses on the DNS

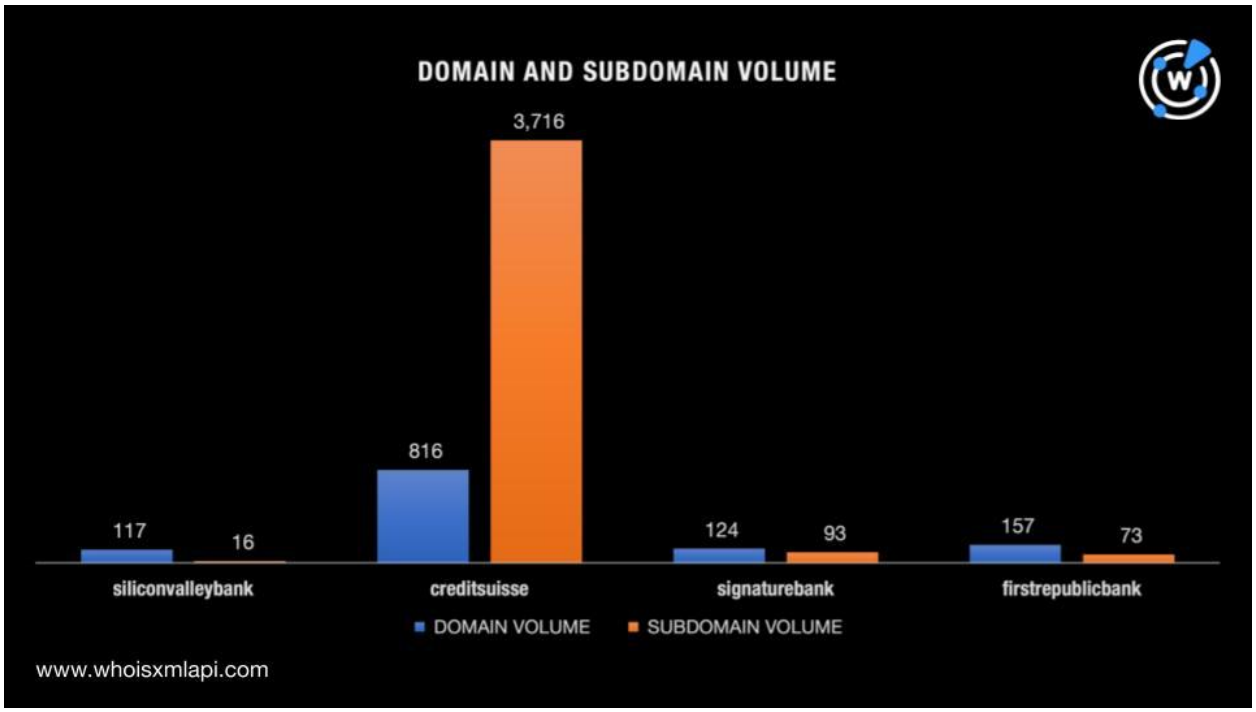
SVB and Credit Suisse weren't the first U.S. banks to collapse in March. Silvergate Capital closed shop on 8 March due to the crypto industry downturn. At that time, SVB investors had already begun selling their shares as depositors withdrew their money. Signature Bank followed suit on 12 March when its investors pulled out. Flagstar Bank and New York Community

Bancorp, however, bought Signature Bank's shares. On 19 March, Credit Suisse closed shop after a botched-up deal with UBS Group AG. While First Republic Bank hasn't shut down per se, it has been affected by large customer withdrawals.

Phishers and other fraudsters are bound to take advantage of each bank's peculiar situation. That said, we sought to discover if their names have figured in malicious campaigns.

Domains & Subdomains Discovery searches for each of the bank's names led to the discovery of 1,220 domains and 3,902 subdomains. The table and chart below show the search strings we used and the domain and subdomain volume breakdown.

Bank	Search String
Silicon Valley Bank	***siliconvalleybank***
Credit Suisse	***creditsuisse***
Silvergate Capital Corp.	***silvergatecapital***
Signature Bank	***signaturebank***
First Republic Bank	***firstrepublicbank***



*Note: **Silvergatecapital** appeared in only six domains and four subdomains.*

A bulk WHOIS lookup for the domains containing the banks' names showed that:

- SVB only owned 21 of the 117 domains that contained its name since they shared svb[.]com's registrant email address.
- Credit Suisse could only be publicly attributed to 51 of the 816 domains that contained its name based on the registrant organization indicated in their WHOIS records.
- Signature Bank only owned 15 of the 124 domains that contained its name since they shared signatureny[.]com's registrant email address.

We couldn't determine how many of the domains containing the names of Silvergate Capital and First Republic Bank were actually owned by the institutions since their WHOIS records were privacy-protected.

Bulk malware checks for the web properties revealed that 23 of them—20 domains and three subdomains to be exact—have already been classified as malicious.

We also looked at the possibility that cybercriminals might jump on the chance to weaponize web properties that contained the string ***bankcollapse*** should a financial crisis indeed ensue. So far, we've only found 31 domains, a majority of which were registered just this year, and one subdomain.

Unsurprisingly, some of them contained ***siliconvalleybank*** or ***svb***, which already closed shop. On the other end of the spectrum, some contained the string ***deutschebank***, which remains in operation and hasn't shown any sign of collapsing whatsoever.

Apart from fake bank collapse news that could be hosted on the 31 domains we found, other dangerous sites containing dire warnings of impending bank closures could litter the Web in the future. Threat actors could thus take advantage of domains containing the strings ***bankalert*** and ***bankupdate***.

We found 278 ***bankalert***- and 124 ***bankupdate***-containing domains to date. Of these, 21 and eight, respectively, turned out to be malicious.

We also uncovered 420 ***bankalert***- and 197 ***bankupdate***-containing subdomains, 12 and 23, respectively, of which have been dubbed malware hosts. The names of Chase Bank, Citibank, and Scotiabank also appeared in some of them.

—

The recent bank collapses have translated into measurable domain activity, as evidenced by the recent additions of domains containing ***bankcollapse***. We're bound to see more such web properties crop up as updates continue to unfold and some of them could bring harm to visitors if not closely monitored and classified.

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 Containing the Featured Banks' Names

- creditsuissecreditsuisse[.]ws
- creditsuisse[.]lk
- creditsuisse[.]be
- creditsuisse[.]as
- xn--crditsuisse-cbb[.]li
- creditsuisse[.]sc
- creditsuisse[.]gr
- creditsuisse[.]cl
- creditsuisse[.]hu
- creditsuisse[.]ai
- creditsuisse[.]nu
- creditsuisse[.]md
- creditsuisse[.]ua
- creditsuisse[.]xn--ses554g
- creditsuisse[.]at
- creditsuisse[.]la
- creditsuisse[.]ch
- creditsuisse[.]au
- creditsuisse[.]mw
- creditsuisse[.]fm
- xn--frstrepublicbank-8rb[.]ws
- xn--firstrepublcbank-moc[.]ws
- xn--firstrepubicbank-syc[.]ws
- xn--frstrepublicbank-ixe[.]ws
- xn--firstrepublicbnk-8nb[.]ws
- xn--firstrepublicbnk-9mb[.]ws
- xn--firstrepublcbank-sxe[.]ws
- xn--firstrepublibank-npb[.]ws
- xn--firstrepulicank-0dgd[.]ws
- firstrepublicbank[.]us
- xn--firstrepulicbank-drg[.]ws
- xn--fistepublicbank-kwgc[.]ws
- firstrepublicbank[.]vg
- xn--firstrpublicbank-qfc[.]ws
- xn--firstrepublibank-64b[.]ws
- xn--firstrepublcbank-jsb[.]ws
- xn--firsrepublicbank-nfd[.]ws
- firstrepublicbank[.]co
- xn--firstrepblicbank-mkd[.]ws
- firstrepublicbank[.]cc
- signaturebank[.]cc
- signaturebank[.]eu
- signaturebank[.]de
- signaturebank[.]us
- signaturebank[.]ltd
- signaturebank[.]biz
- signaturebank[.]nyc
- signaturebank[.]xyz
- signaturebank[.]vip
- signaturebank[.]one
- signaturebanks[.]eu
- signaturebank[.]org
- signaturebank[.]com
- signaturebank[.]net
- signaturebank[.]app
- 1signaturebank[.]com

- signaturebank[.]bank
- signaturebankmi[.]tv
- signaturebankna[.]co
- signaturebanks[.]com
- siliconvalleybank[.]xn--kprw13d
- siliconvalleybank[.]cn
- siliconvalleybank[.]ca
- siliconvalleybank[.]fr
- siliconvalleybank[.]ga
- siliconvalleybank[.]uk
- siliconvalleybank[.]se
- siliconvalleybank[.]nu
- siliconvalleybank[.]de
- siliconvalleybank[.]us
- siliconvalleybank[.]run
- siliconvalleybank[.]com
- siliconvalleybank[.]biz
- siliconvalleybank[.]net
- siliconvalleybank[.]xyz
- siliconvalleybank[.]lol
- siliconvalleybank[.]org
- siliconvalleybank[.]asia
- siliconvalleybank[.]wine
- siliconvalleybank[.]site
- siliconvalleybanksettlement[.]com
- siliconvalleybankclasaction[.]com
- siliconvalleybanktradeclaim[.]com
- siliconvalleybankukltd[.]financial
- siliconvalleybankclassaction[.]com
- siliconvalleybankruptcylawyer[.]com
- siliconvalleybankruptcylawyers[.]com
- siliconvalleybankruptcyattorney[.]com
- wwwsiliconvalleybankclassaction[.]com
- continentofsiliconvalleybanking[.]com
- siliconvalleybankruptcyattorneys[.]com
- siliconvalleybankcustomerservice[.]com
- siliconvalleybankownedrealestate[.]com
- siliconvalleybankreceivershipcertificate[.]com
- silvergatecapital[.]ca
- silvergatecapital[.]com
- silvergatecapital[.]ltd
- silvergatecapitals[.]ltd
- silvergatecapitalgroup[.]com
- silvergatecapitalcooperation[.]com

Sample Malicious Domains Containing the Featured Banks' Names

- xn--crditsuisse-cbb[.]dk
- creditsuisse[.]icu
- creditsuisses[.]com
- creditsuisse-ag[.]com
- thecreditsuisse[.]com
- creditsuissecpa[.]com
- intcreditsuisse[.]com
- creditsuisse[.]online
- creditsuisseint[.]com
- creditsuisse-usa[.]com

Sample Subdomains Containing the Featured Banks' Names

- creditsuissemt4creditsuisselphcreditsuisse[.]foxycart[.]com
- creditsuisse-creditsuisse[.]foxycart[.]com
- creditsuisse-creditsuisse[.]workday[.]in
- creditsuissembcreditsuissesscreditsuissedor[.]foxycart[.]com

- creditsuissei8creditsuisse[.]foxycart[.]com
- andrewcreditsuisse-lab-acreditsuissecreditsuisseetcreditsuisse[.]foxycart[.]com
- 2acreditsuissecreditsuisses[.]foxycart[.]com
- adscreditsuisservcreditsuisser-creditsuisseast[.]foxycart[.]com
- acreditsuissecreditsuissea-6[.]foxycart[.]com
- 3mcreditsuissembcreditsuissers-bcreditsuisseta[.]foxycart[.]com
- acreditsuissecreditsuisseeptatie-creditsuissehef[.]foxycart[.]com
- aerospcreditsuissee-ncreditsuissecreditsuissehe[.]foxycart[.]com
- creditsuisselphcreditsuissedevel-betcreditsuisse[.]foxycart[.]com
- afvcreditsuissec1creditsuisse[.]foxycart[.]com
- afccreditsuissert-crcreditsuissedockcreditsuisser[.]foxycart[.]com
- creditsuissemis-screditsuisset[.]foxycart[.]com
- creditsuisse[.]vk[.]cc
- creditsuisse[.]info[.]nr
- creditsuisse[.]relatelq[.]com
- creditsuisse[.]app[.]link
- firstrepublicbank[.]affinio[.]com
- firstrepublicbank[.]demdex[.]net
- firstrepublicbank[.]bitrix24[.]com
- firstrepublicbank[.]ed[.]pw
- firstrepublicbank[.]netflixawards[.]com
- firstrepublicbank[.]kriscargologistics[.]com
- firstrepublicbank[.]advice[.]financial
- firstrepublicbank[.]werecognize[.]com
- firstrepublicbank[.]mktoweb[.]com
- firstrepublicbank[.]sc[.]fallguys-show[.]com
- firstrepublicbank[.]tt[.]kinderjoycrazyfriendsroadshow[.]eu
- firstrepublicbank[.]tt[.]jogurt-slice[.]com[.]pl
- firstrepublicbank[.]tt[.]1password[.]ca
- firstrepublicbank[.]sc[.]irregularcorporation[.]com
- firstrepublicbank[.]tt[.]witaj-szkolo-na-wesolo[.]eu
- firstrepublicbank[.]tt[.]omtrdc[.]net
- firstrepublicbank[.]sc[.]fallguys2[.]com
- firstrepublicbank[.]tt[.]kindermaxi[.]nl
- firstrepublicbank[.]jm[.]encoremerchants[.]com
- firstrepublicbank[.]sc[.]tictac-breeze[.]cz
- signaturebank[.]csinufund[.]com
- signaturebank[.]wpenginepowered[.]com
- signaturebank[.]or[.]pw
- signaturebank[.]framer[.]website
- signaturebank[.]federalcreditbreach[.]com
- signaturebank[.]safeconsolecloud[.]io
- signaturebank[.]mymortgage-online[.]com
- signaturebank[.]snowflake-analytics[.]com
- signaturebank[.]belau[.]pw
- signaturebank[.]secure-citrix[.]com
- signaturebank[.]livemeetinginvite[.]com
- signaturebank[.]wpengine[.]com
- signaturebank[.]hitta[.]se

- signaturebank[.]humio[.]cloud
- signaturebank[.]lamabanking[.]com
- signaturebank[.]zendesk[.]com
- signaturebankga[.]insuranceaisle[.]com
- signaturebankna[.]lenderscooperative[.]com
- signaturebankga[.]as[.]me
- signaturebankga[.]onlineportalnow[.]com
- siliconvalleybank[.]co[.]xyz
- siliconvalleybank[.]mktoweb[.]com
- siliconvalleybank[.]co[.]com[.]au
- siliconvalleybank[.]avonow[.]com
- siliconvalleybank[.]oathello[.]com
- svbsiliconvalleybank[.]xn--55qx5d[.]cn
- www[.]siliconvalleybank[.]oathello[.]com
- siliconvalleybankukltd[.]co[.]xyz
- siliconvalleybankukltd[.]co[.]com[.]au
- siliconvalleybanksharkfrenzy[.]splashthat[.]com
- siliconvalleybank[.]julstoreusprosites[.]kinsta[.]cloud
- siliconvalleybankers-com[.]mail[.]protection[.]outlook[.]com
- siliconvalleybank[.]innovid[.]julstoreusprosites[.]kinsta[.]cloud
- siliconvalleybank[.]complex[.]julstoreusprosites[.]kinsta[.]cloud
- siliconvalleybank[.]contentsquare[.]julstoreusprosites[.]kinsta[.]cloud
- siliconvalleybank[.]carbonlighthouse[.]julstoreusprosites[.]kinsta[.]cloud
- silvergatecapital[.]ltd[.]global-financehub[.]com
- silvergatecapitals[.]ltd[.]global-financehub[.]com
- www[.]silvergatecapital[.]ltd[.]global-financehub[.]com
- www[.]silvergatecapitals[.]ltd[.]global-financehub[.]com
- creditsuisse[.]demdex[.]net
- creditsuisse[.]stitched[.]io
- creditsuisse[.]quadram[.]mobi
- creditsuisse[.]wealthtouch[.]com
- creditsuisse[.]netflox[.]ca
- creditsuisse[.]justeat[.]it
- adminsicreditsuissees-screditsuisseagecreditsuisse[.]foxycart[.]com
- creditsuisse[.]telefonoatencion11881[.]com
- creditsuisse[.]okta[.]com
- creditsuisse[.]qjctpm[.]com
- creditsuisse[.]nutella[.]com[.]pl
- creditsuisse[.]realtime[.]email
- creditsuisse[.]talkwalker[.]app
- creditsuisse[.]globalipaction[.]ch
- creditsuisse[.]ivalua[.]com
- creditsuisse[.]lafourchette[.]com
- creditsuisse[.]wellbeingzonestaging[.]co[.]uk
- creditsuisse[.]fehradvice[.]com
- creditsuisse[.]wetransfer[.]com
- creditsuisse[.]banklocationmaps[.]com

Sample Malicious Subdomains Containing the Featured Banks' Names

- creditsuisse[.]ucqhnv[.]com
- firstrepublicbank[.]sc[.]ns32[.]kinderramadan[.]com

Sample Domains Containing the String *bankcollapse*

- collapsebank[.]com
- bankcollapse[.]pro
- bankcollapse[.]com
- svbankcollapse[.]com
- thebankcollapse[.]com
- bankingcollapse[.]com
- bigbankcollapse[.]com
- collapsebanking[.]com
- bankcollapse2023[.]com
- bankcollapseapp[.]info
- bankcollapse[.]capital
- 2023bankcollapse[.]com
- bankcollapselawyer[.]com
- bankingcollapseinu[.]com
- deutschebankcollapse[.]fm
- 2023bankingcollapse[.]com

Sample Domains Containing the String *bankalert*

- bankalert[.]co
- bankalert[.]ru
- bankalert[.]ci
- bankalert[.]in
- bankalert[.]me
- bankalert[.]tk
- bankalerts[.]co
- bankalert[.]org
- bankalert[.]app
- bankalerts[.]in
- bankalert[.]com
- bankalerts[.]id
- bankalert[.]one
- bankalert[.]net
- bankalert[.]biz
- bankalert[.]xyz
- bankalert[.]win
- mtbankalert[.]cf
- bankalert[.]asia
- bankalerts[.]net
- bankalerts[.]com
- ebankalert[.]com
- akbankalert[.]ph
- bankalerts[.]win
- mtbankalert[.]tk
- mtbankalert[.]ga
- akbankalert[.]la
- mtbankalert[.]ml
- bankalert[.]club
- mybankalert[.]ru
- bankalerts[.]xyz
- bankalertt[.]com
- bankalert[.]mobi
- bankalert[.]info
- bankalertz[.]com
- usbankalert[.]xyz
- usbankalert[.]com
- reobankalert[.]vg
- bankalertss[.]com
- bankalert[.]space
- bankalert[.]cloud
- bankalerts[.]mobi
- mrbankalert[.]com
- pncbankalert[.]tk
- bankalertng[.]com
- mtbankalert[.]com
- ingbankalert[.]vg
- bankalerts[.]live
- bankalertsp[.]com
- bankalert[.]co[.]uk

Sample Malicious *bankalert*-Containing Domains

- bankalert[.]ci
- bankalerts[.]net

- bankalertt[.]com
- pncbankalert[.]tk
- netbankalert[.]com
- ingbankalert[.]info
- commbankalert[.]app
- ingbankalerts[.]info
- inlandbankalert[.]org
- citizenbankalert[.]us
- bendigobankalert[.]com

Sample Subdomains Containing the String *bankalert*

- bankalert[.]kindercrazyfriends[.]com[.]pl
- bankalert[.]newsnaira[.]com
- bankalert[.]personio[.]de
- bankalert[.]thewoxserver[.]com
- bankalert[.]vitbank[.]com
- bankalert[.]kinderjoycrazyfriends[.]pl
- bankalert[.]freshnow[.]org[.]pl
- bankalert[.]spacelander[.]co[.]in
- bankalert[.]kinder-paradiso[.]cz
- bankalert[.]fallguys2d[.]com
- bankalert[.]fallguysultimateknockout[.]net
- bankalert[.]minikinderbueno[.]net[.]pl
- bankalert[.]gcr[.]io
- bankalert[.]fallguys[.]global
- bankalert[.]fallguys-movie[.]net
- bankalert[.]netfli[.]ca
- bankalert[.]kinderbueno[.]ch
- bankalert[.]vitrineartsetdecor[.]com
- bankalert[.]roadshowzabawanacalego[.]com[.]pl
- bankalert[.]soc-club[.]ru
- bankalert[.]fallguys-mobile[.]com
- bankalert[.]fallguysmusic[.]net
- bankalert[.]fallguystwo[.]com
- bankalert[.]fallguys2[.]com
- bankalert[.]kindercountry[.]com[.]pl
- bankalert[.]bitrix24[.]com
- bankalert[.]8x8[.]vc
- bankalert[.]fallguys-shop[.]com
- bankalert[.]yelp[.]com
- bankalert[.]officient[.]io
- bankalert[.]withthegrid[.]com
- bankalert[.]nutella[.]com[.]pl
- bankalert[.]rondnoir[.]cz
- bankalerts[.]zalando-prive[.]be
- bankalerts[.]ferreroduplo[.]pl
- bankalerts[.]raffaello[.]sk
- bankalerts[.]kinderjoyzabawanacalego[.]eu
- bankalerts[.]yogurt-slice[.]pl
- bankalerts[.]joghurtschnitte[.]cz
- bankalerts[.]drfred[.]xyz
- bankalerts[.]kinderbuenowhite[.]info
- bankalerts[.]housepartyfun[.]com
- bankalerts[.]kinderpingui[.]com[.]pl
- bankalerts[.]fallguys3d[.]com
- bankalerts[.]crazyfriendszabawanacalego[.]pl
- bankalerts[.]kindermlecznakanapka[.]com
- bankalerts[.]fallguys-shop[.]com
- bankalerts[.]roadshowcrazyfriends[.]eu
- bankalerts[.]freshnow[.]com[.]pl
- bankalerts[.]pocketcoffee[.]ch

Sample Malicious *bankalert*-Containing Subdomains

- mtbankalert[.]jkub[.]com
- mtbankalert[.]serveirc[.]com

- mtbankalert[.]duckdns[.]org
- mntbankalerts[.]duckdns[.]org
- usaabankalerts[.]duckdns[.]org
- 1firstbankalert[.]pages[.]dev
- region-bankalert[.]duckdns[.]org

Sample Domains Containing the String *bankupdate*

- bankupdate[.]co
- bankupdate[.]tk
- bankupdate[.]gq
- bankupdate[.]in
- bankupdate[.]us
- bankupdatez[.]in
- bankupdates[.]in
- bankupdate[.]xyz
- bankupdate[.]com
- bankupdate[.]net
- bankupdates[.]nl
- bankupdates[.]net
- bankupdates[.]com
- ibankupdate[.]com
- bankupdate[.]info
- usbankupdate[.]ml
- bankupdates[.]org
- svbankupdate[.]com
- ingbankupdate[.]ph
- bankupdates[.]info
- usbankupdate[.]com
- mtbankupdate[.]com
- ingbankupdate[.]ws
- dzbankupdates[.]com
- bankupdates[.]co[.]in
- burbankupdate[.]com
- bankupdate[.]online
- mtbankupdate[.]live
- combankupdate[.]com
- keybankupdate[.]net
- us-bankupdate[.]com
- usabankupdate[.]com
- keybankupdate[.]com
- axabankupdaten[.]xyz
- seedbankupdate[.]com
- aktifbankupdate[.]ph
- infobankupdate[.]com
- icicibankupdate[.]tk
- citibankupdate[.]com
- landbankupdate[.]org
- chasebankupdate[.]cf
- turkbankupdate[.]xyz
- redbankupdates[.]com
- commbankupdate[.]com
- aktifbankupdate[.]vg
- metro-bankupdate[.]ml
- wellsbankupdate[.]com
- wellsbankupdate[.]net
- comm-bankupdate[.]com
- metrobankupdate[.]xyz

Sample Malicious *bankupdate*-Containing Domains

- bankupdate[.]gq
- bankupdate[.]us
- bankupdate[.]net
- combankupdate[.]com

Sample Subdomains Containing the String *bankupdate*

- bankupdate[.]swansonsteamfresh[.]ca
- bankupdate[.]on5[.]biz
- bankupdate[.]omnicard[.]com
- bankupdate[.]okta[.]com
- bankupdate[.]elvenar[.]com

- bankupdate[.]preferredcredit[.]net
- bankupdate[.]modeso[.]ch
- bankupdate[.]pulleyapp[.]com
- bankupdate[.]simplenote[.]com
- bankupdates[.]finance[.]blog
- bankupdates[.]azurewebsites[.]net
- mtbankupdate[.]diskstation[.]eu
- rcbankupdate[.]kwiksoftware[.]in
- mtbankupdate[.]duckdns[.]org
- mybankupdates[.]great-site[.]net
- www[.]bankupdate[.]instructure[.]com
- www[.]bankupdate[.]omnicard[.]com
- www[.]bankupdate[.]preferredcredit[.]net
- fbmebankupdate[.]startupdate[.]nl
- usaabankupdate[.]seniors-australia[.]com
- www[.]bankupdate[.]acretrader[.]com
- fbmebankupdate[.]startfreak[.]nl
- bankupdate[.]acc[.]mobilevikings[.]be
- www[.]bankupdate[.]netflox[.]ca
- goldbankupdate[.]finance[.]blog
- fbmebankupdate[.]gigastart[.]nl
- www[.]bankupdate[.]nerflix[.]ca
- www[.]bankupdate[.]faraday[.]io
- stbankupdateqa[.]worldbank[.]org
- mntbankupdate2[.]x24hr[.]com
- citibankupdate[.]account-tmobile[.]com
- fbmebankupdate[.]linkhaven[.]nl
- bankupdate[.]net[.]verification[.]com[.]ng
- allbankupdates[.]tummart[.]com
- mntbankupdate1[.]servebeer[.]com
- www[.]bankupdate[.]connxusdemo[.]com
- www[.]bankupdates[.]finance[.]blog
- chasebankupdate[.]upgradeserviceform[.]com[.]ng
- bankupdate[.]link[.]vantiv[.]com
- fbmebankupdates[.]weebly[.]com
- clickbankupdate[.]finance[.]blog
- wellsbankupdate[.]aussievitamin[.]com
- erstebankupdate[.]web[.]app
- alphabankupdate[.]soggiornasalerno[.]com
- clickbankupdates[.]turbocashprofits[.]com
- latestbankupdate[.]bokundemo[.]com
- latestbankupdate[.]staging-airtableblocks[.]com
- latestbankupdate[.]williamhill[.]com
- latestbankupdate[.]dyson[.]at
- latestbankupdate[.]miro[.]com

Sample Malicious *bankupdate*-Containing Subdomains

- mtbankupdate[.]diskstation[.]eu
- mtbankupdate[.]duckdns[.]org
- mybankupdates[.]great-site[.]net
- www[.]mtbankupdate[.]duckdns[.]org
- usbankupdate-023[.]serveuser[.]com
- mail[.]mtbankupdate[.]duckdns[.]org
- www[.]mybankupdates[.]great-site[.]net
- cpanel[.]mtbankupdate[.]duckdns[.]org
- webmail[.]mtbankupdate[.]duckdns[.]org
- webdisk[.]mtbankupdate[.]duckdns[.]org

- citibankupdate-secunw[.]dynamic-dns[.]net
- westamericabankupdate[.]duckdns[.]org