Are Threat Actors Intercepting Your OTPs? These Cyber Resources Might Be Helping Them

Table of Contents

Executive Report

A group of researchers recently discovered a new Android banking Trojan they called "Revive" since threat actors designed it to restart if it stops working. Once a device is infected, hackers can intercept messages, including online banking one-time passwords (OTPs). Revive also enables attackers to steal login credentials since it can read and store everything the user types on the infected device.

Although new, Revive uses age-old phishing tactics, including look-alike domains and web pages. We looked into the indicators of compromise (IoCs) mentioned in the report and expanded these to uncover more artifacts that could potentially be used to deliver the malware. Our findings include:

- 3,300+ cyber resources that use the text strings "bbva," "2fa + app," "2fa + secure," and "app + secure"
- Only 18% of these properties actively resolved to IP addresses
- About 7% of the cyber resources have been flagged as malicious, most of which contained the string "bbva"
- While most of the resolving properties were parked or hosted 404 pages, 6% led to login pages

We discussed the details of our findings below.

What We Know about the IoCs

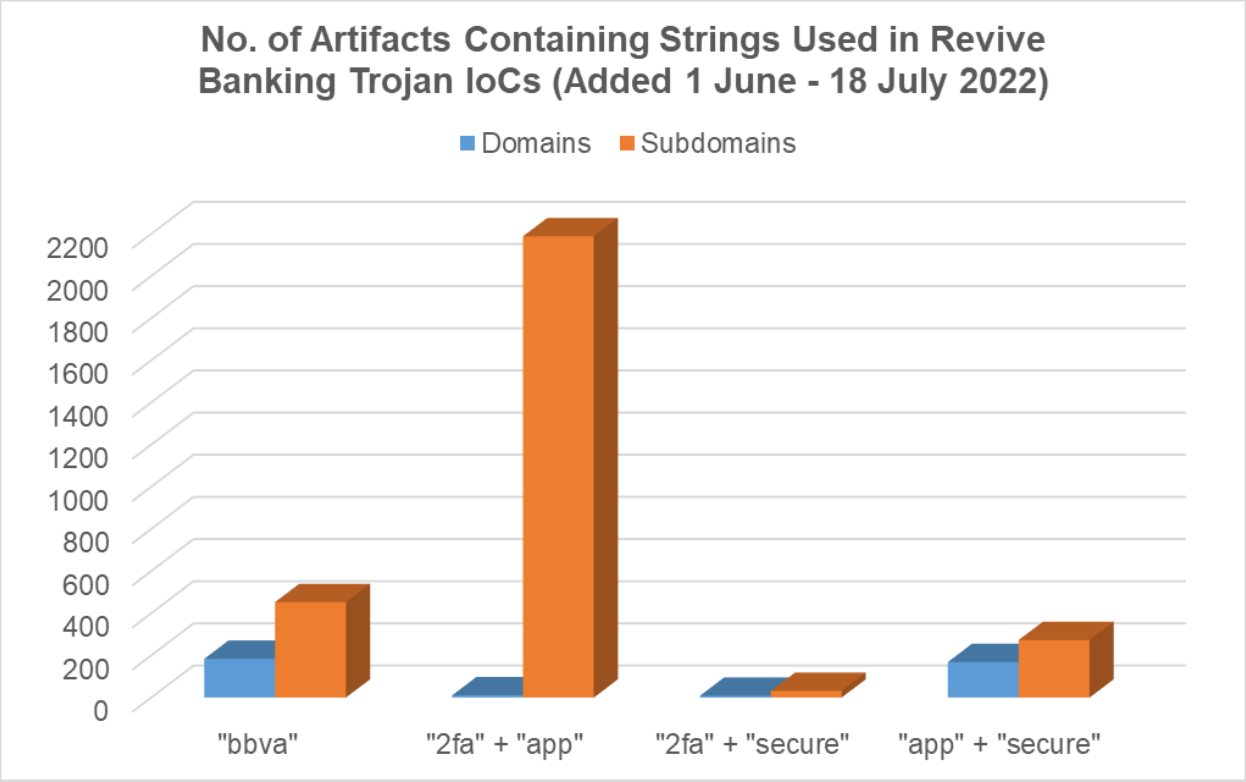
Two phishing domains were used to deliver the malware when it was detected on 15 June 2022. These were bbva[.]european2fa[.]com and bbva[.]appsecureguide[.]com, both imitating

the Spanish financial services company, Banco Bilbao Vizcaya Argentaria, S.A. (BBVA) whose official domain is bbva[.]com.

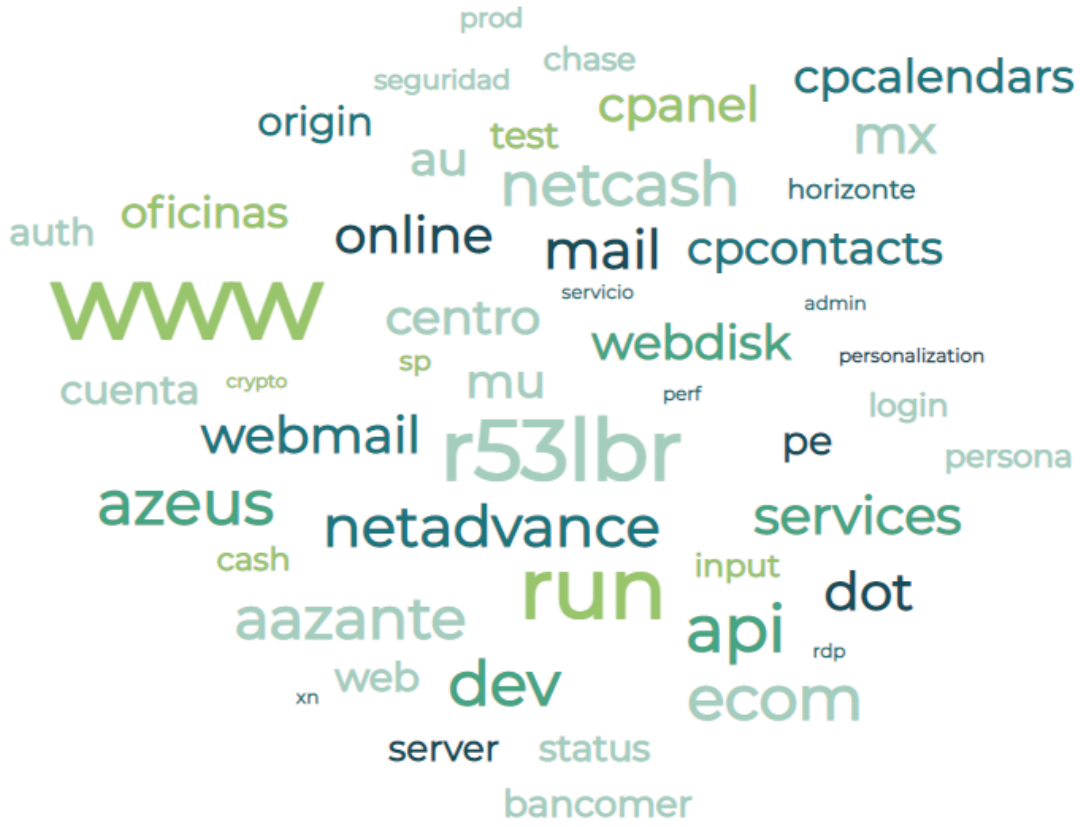
WHOIS Lookup revealed that both IoCs were newly registered domains (NRDs), having been so only on 8 and 15 June 2022, respectively. The domain bbva[.]european2fa[.]com is managed by OwnRegistrar, while the other by NameSilo. The two IoCs had privacy-protected WHOIS records.

Thousands of BBVA and 2FA Digital Properties Added Since June 2022

Using Domains & Subdomains Discovery, we looked for other properties containing some of the text strings used in the IoCs. We found 3,320 cyber resources. The chart below shows how these were distributed across the different search strings.

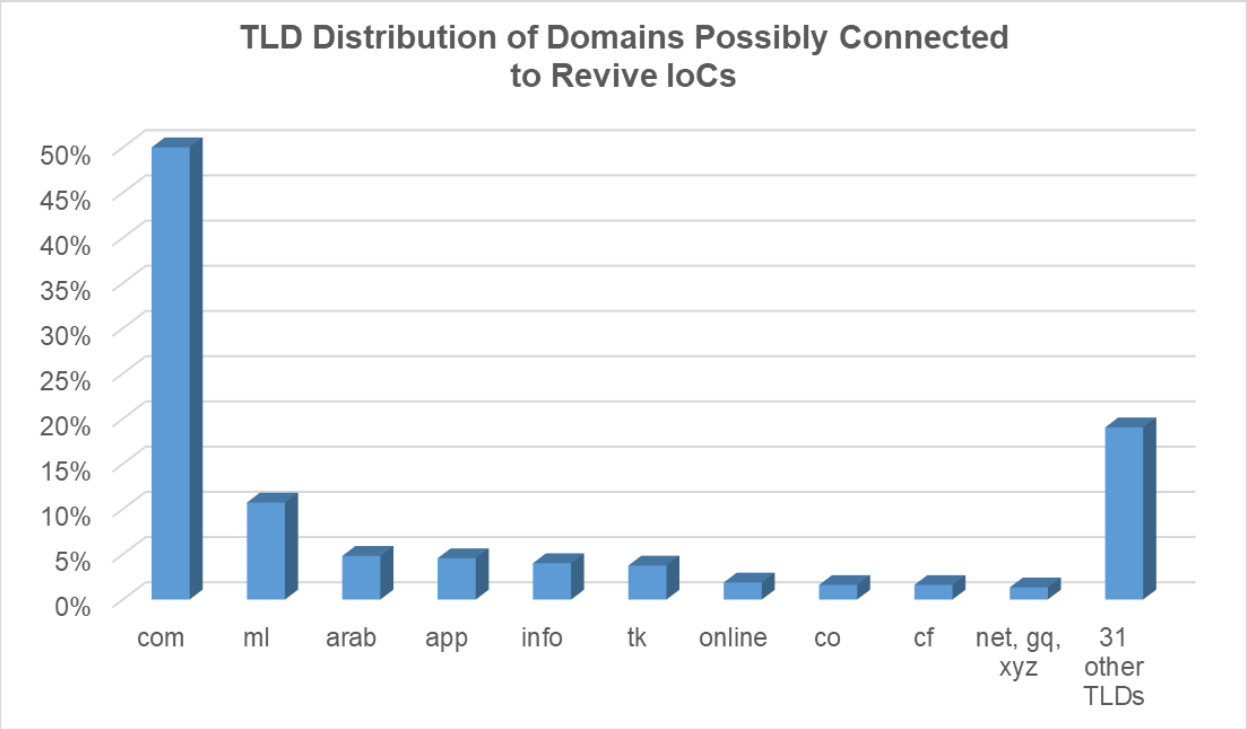


Aside from these text strings, other words that repeatedly appeared in the artifacts included “services,” “mail,” “login,” and “online.” Dozens of properties also seemed to imitate Chase. These and other strings can be seen in the word cloud below.



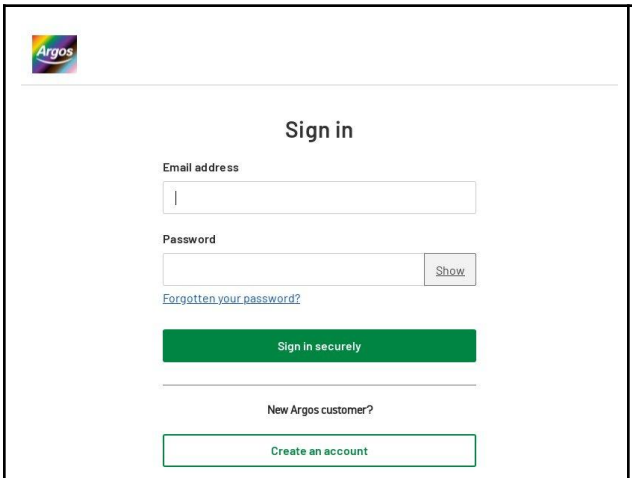
Based on the [Bulk IP Lookup results](), only 18% of the more than 3,000 artifacts actively resolved to 487 unique IP addresses.

On the other hand, half of the domains in the sample fell under the .com top-level domain (TLD). It was followed by .ml (11%) and .arab and .app (5% each). The chart below shows the TLD distribution of the domains connected to the Revive IoCs based on text strings.

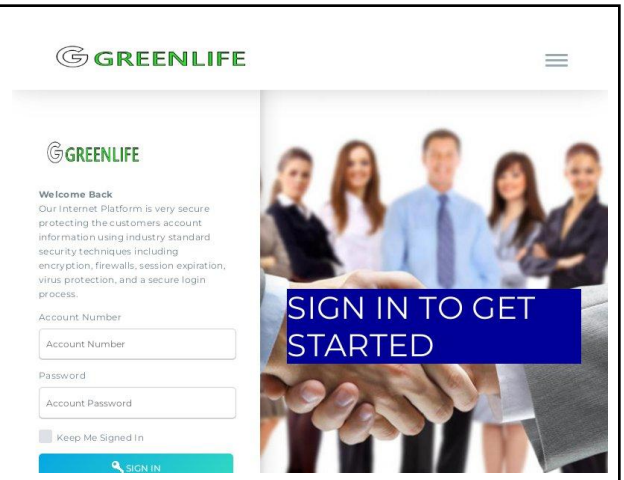


What Types of Content Do the Artifacts Host?

Screenshot analyses of the resolving properties proved interesting. About 6% showed login pages, some of which were pretty suspicious. Examples include properties imitating Argos Card and a company named "Greenlife." The researchers' browser security blocked access to both pages.



Screenshot of www[.]argoscardsecureappupdate-mobileonlineupdate[.]online[.]iiscnet[.]in



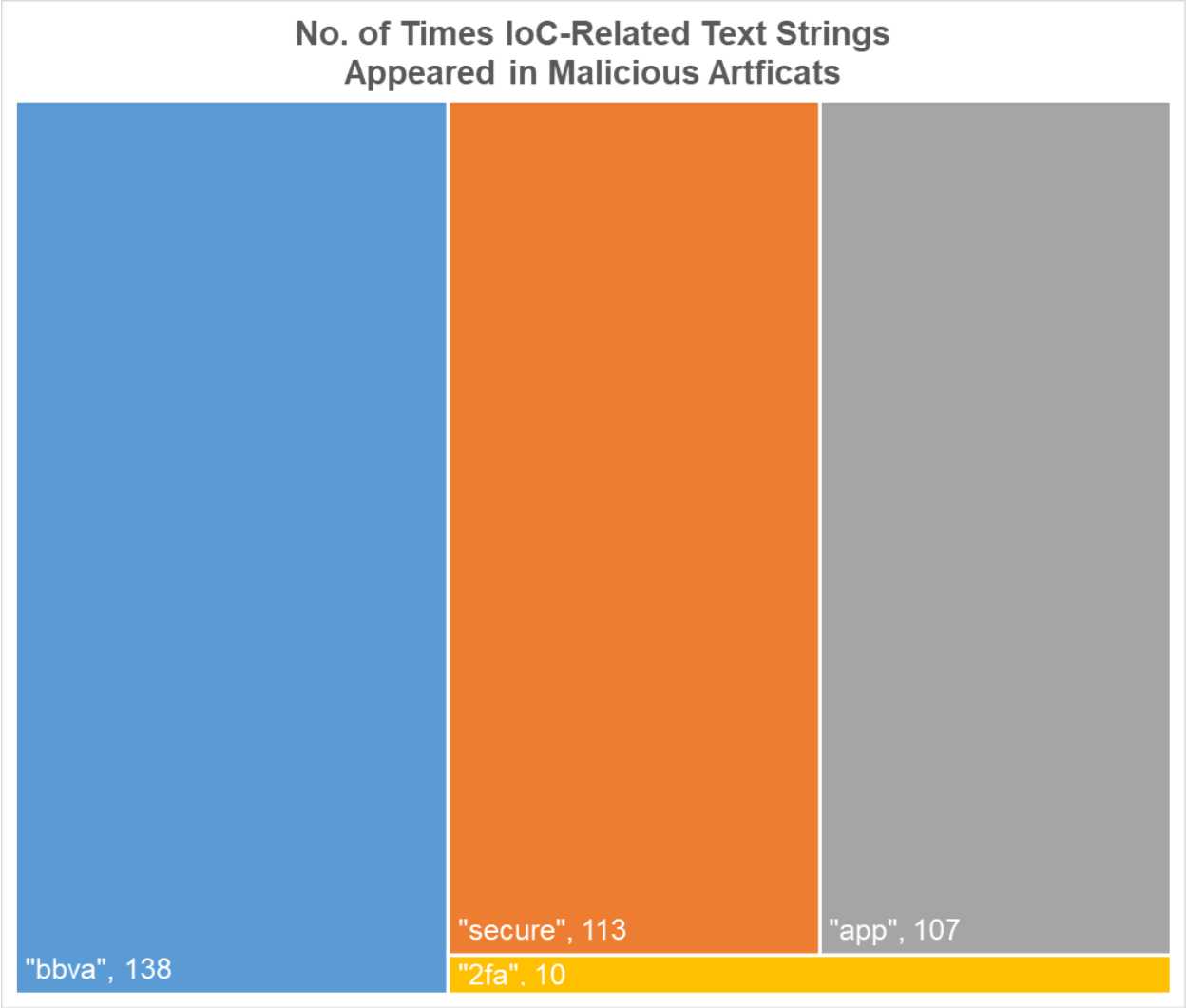
Screenshot of app[.]greenlife-secure[.]bk-llc[.]info

Other properties were either parked or resolved to 404 and index pages. However, one domain—bbvaallianzsegurospt[.]soportedigital[.]es—stood out since it hosted a look-alike of the BBVA homepage and was blocked by the researchers' antimalware.

Screenshot of bbvaallianzsegurospt[.]soportedigital[.]es

Malicious Artifacts Uncovered

Hundreds of artifacts have already been reported as malicious by various malware engines. Specifically, 7% of the properties were malicious. We broke down the number of times the text strings in the Revive IoCs appeared in the malicious artifacts. We found that "bbva" recurred most, followed by "secure" and "app." The distribution is reflected in the chart below.



—

Revive and other banking Trojans can lead to the loss of people's hard-earned money. Along with implementing two-factor authentication (2FA), monitoring and blocking access to potential malware carriers can help protect individuals and companies.

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 Domains Added Since 1 June 2022

- 2022garantibbvahediyeleri[.]ml
- 24personalbbva[.]com
- 2b2fapparel[.]net
- 2fa-app[.]buzz
- 2fa-app[.]com
- 2fa-app[.]digital
- 2fa-app[.]info
- 2fa-app[.]live
- 2fa-app2[.]com
- amazon-com-secure-recovery-reff2f a282hdc[.]tk
- anulacion-bbva[.]info
- anulacion-bbva-recibo[.]info
- anulaciones-bbva[.]info
- app-1secure[.]com
- app2fa-mobile[.]digital
- app-2secure[.]com
- app-authsecure[.]com
- app-chainlisst-secure[.]com
- appdigitalsecure[.]com
- bbva-services[.]ml
- bbvaservicio[.]info
- bbvaservicio[.]net
- secure-id8647-apple[.]com
- secure-id8693-apple[.]com
- secure-id9863-apple[.]com
- secureid-app[.]com
- secure-login-anz[.]app
- securemainappnet[.]com
- secure-meapp[.]xyz
- secure-mobileapproval[.]com
- tesgaihubbvatma[.]gq
- thewebsecureappaccount[.]ws
- tradesun-bbvape[.]com
- tvbappsecuremailalertidinfo[.]com
- userssecure2fa[.]com
- uubbvaxi[.]arab
- vaxbbvagff[.]fun
- vbbvanetcahs[.]com
- vedigobbvamocor[.]tk
- verificacion-bbva[.]com
- verificarbbvaonline[.]arab
- verification-secure-app[.]com
- wells-appsecure[.]com
- wells-secure01app[.]com
- wjrlockappsecuremailaccidamazon[.]com
- wvvvv-app2fa[.]com
- www03bbvanet[.]arab
- wwwbbvavivienda[.]arab
- xn--garantibbv-nj3e[.]com
- xn--verificacin-bbva-fvb[.]com

Sample Subdomains Added Since 1 June 2022

- bbva[.]accesoportalweb[.]com
- bbva[.]actualizacion-cliente[.]ml
- bbva[.]aplicacion-descargar[.]ru
- bbva[.]aplicacion-es[.]com
- bbva[.]aplicacion-seguridad[.]online
- bbva[.]app-movil[.]icu
- bbva[.]app-protect[.]click
- bbva[.]app-protect[.]info
- bbva[.]app-protect[.]top
- bbva[.]appsecure2fa[.]com

- bbva[.]appsecureguide[.]com
- bbva[.]area-clientes[.]ga
- bbva[.]auth-id-30[.]com
- bbva[.]bankacceso[.]com
- bbva[.]cageret[.]leitungsen[.]de
- bbva[.]cargos-registro[.]info
- bbva[.]centro-online-atencion[.]com
- bbva[.]com[.]ar[.]admin-mcas-df[.]ms
- bbva[.]com[.]ar[.]mcas-df[.]ms
- bbva[.]com[.]co[.]admin-mcas-df[.]ms
- chase-securedapps[.]vantechdns[.]com
- chase-secureverifyesdetailsapps[.]vantechdns[.]com
- cihp1swwdhcamji[.]www[.]blog[.]beta[.]dev[.]applicationsecure[.]neraplatform[.]com
- citibank[.]com[.]secure-application[.]session[.]ssn-php[.]one
- citit-secure2facclogonn[.]serveusers[.]com
- ckbdxavqbe6v5h7mmk7p7bbvaq[.]me-south-1[.]es[.]amazonaws[.]com
- cliente-bbva-colectivos-bbvaoficinas-bbva[.]misecure[.]com
- cobbvanthdilf[.]carrd[.]co
- cohttpdjzbbvafnujh[.]planeta-s[.]ru
- cohttwww[.]pdjzbbvafnujh[.]planeta-s[.]ru
- community-bbvabancomer[.]assima[.]net
- cpanel[.]app[.]greenlife-secure[.]bk-llc[.]info
- cpanel[.]apppayidonsecureid[.]cloudns[.]ph
- cpanel[.]appsecurecitizens8531[.]duckdns[.]org
- cpanel[.]authsecure2fa-accountservice[.]duckdns[.]org
- cpanel[.]secure05-chasappsid[.]duckdns[.]org
- cpanel[.]secure062applid[.]duckdns[.]org
- cpanel[.]secure-account2faacconts[.]duckdns[.]org
- cpanel[.]secure-ctzns-2fa[.]duckdns[.]org
- cpanel[.]securewellsappid[.]duckdns[.]org
- cpcalendars[.]apppayidonsecureid[.]cloudns[.]ph
- cpcalendars[.]appsecurecitizens8531[.]duckdns[.]org
- cpcalendars[.]authsecure2fa-accountservice[.]duckdns[.]org
- cpcalendars[.]secure05-chasappsid[.]duckdns[.]org
- cpcalendars[.]secure062applid[.]duckdns[.]org
- cpcalendars[.]secure-account2faaccconts[.]duckdns[.]org
- cpcalendars[.]secure-ctzns-2fa[.]duckdns[.]org
- cpcalendars[.]securewellsappid[.]duckdns[.]org
- cpcontacts[.]apppayidonsecureid[.]cloudns[.]ph
- cpcontacts[.]appsecurecitizens8531[.]duckdns[.]org
- mail[.]apppayidonsecureid[.]cloudns[.]ph
- mail[.]appsecurecitizens8531[.]duckdns[.]org
- mail[.]authsecure2fa-accountservice[.]duckdns[.]org
- mail[.]fix-bbva-for-cci[.]review-me[.]xyz

- mail[.]netflix-2fa-security-secureserver[.]misecure[.]com
- mail[.]secure05-chasappsid[.]duckdns[.]org
- mail[.]secure062applid[.]duckdns[.]org
- mail[.]secure-account2faacconts[.]duckdns[.]org
- mail[.]secure-ctzns-2fa[.]duckdns[.]org
- mail[.]securewellsappid[.]duckdns[.]org
- mbbbva7faqc2ld6oruzyooacki[.]us-west-2[.]es[.]amazonaws[.]com
- merchant-portal[.]bbva[.]qa[.]rubean[.]io
- moviles-bbva[.]aspendigital[.]com[.]br
- moviles-bbva[.]es[.]recursospositivos[.]com
- mxbbva[.]losvientoslogistics[.]com
- myappbtsecurebusiness[.]github[.]io
- nasaapp2015[.]macstechncdn-3[.]test[.]secure[.]pferdezahn-rachel[.]de
- nasaapp2015[.]macstechncdn-3[.]www[.]test[.]secure[.]pferdezahn-rachel[.]de
- netflix-2fa-security-secureserver[.]misecure[.]com
- newsecureaml-devcafjwt[.]centralus[.]cloudapp[.]azure[.]com
- njbbvapsp6av[.]win[.]eng[.]vzwnet[.]com
- njbbvapsp6bv[.]win[.]eng[.]vzwnet[.]com
- njbbvapsp7av[.]win[.]eng[.]vzwnet[.]com
- njbbvapsp7bv[.]win[.]eng[.]vzwnet[.]com
- notification-v-1-0-1-dot-parking-dot-bbva-carparkbooking-mx[.]appspot[.]com
- ocv-secure-development-sf-test[.]southcentralus[.]cloudapp[.]azure[.]com
- officesecuredfiller-app-7ptqp[.]ondigitalocean[.]app
- oficinas-centro2-fnancieras-bbva-info[.]misecure[.]com
- oficinas-centro-ayuda-bbva-cuenta-online[.]4nmn[.]com
- oficinas-centro-bbva-institucion-financiera[.]4nmn[.]com
- oficinas-centro-bbva-institucion-financiera[.]misecure[.]com
- oficinas-centro-bbva-institucion-financiera[.]squirly[.]info
- okufiarurbbvatxalgjsy4ertm[.]ap-southeast-2[.]es[.]amazonaws[.]com
- onboarding-status-service[.]bbva[.]qa[.]rubean[.]io
- online-clientecertificate-bbvainstituciones-es[.]misecure[.]com
- online-clientecertificate-bbva-privada[.]misecure[.]com
- online-cliente-movil-colectivos-bbva[.]misecure[.]com
- oybribbvar[.]ctn[.]gts[.]multisan[.]pr[.]ap[.]gtr[.]certsbridge[.]com
- p4bbvasxarplxgodxwqkkvvspm[.]us-west-2[.]es[.]amazonaws[.]com
- palgwwbcntxbbvaucxaa[.]gtr[.]ing[.]gke[.]certsbridge[.]com
- paymentappsecureid0562[.]duckdns[.]org
- payment-status-service[.]bbva[.]qa[.]rubean[.]io
- perso[.]bbva[.]qa[.]rubean[.]io

- personal[.]bbvaes[.]loginclientea[.]mulasfer[.]leitungsen[.]de
- personal[.]bbvaes[.]loginclienteb[.]caradertva[.]lebtimnetz[.]de
- personal[.]bbvaes[.]loginclienteb[.]hulakiposder[.]leitungsen[.]de
- personal[.]bbvaes[.]loginclienteb[.]judertupola[.]leitungsen[.]de
- personal[.]bbvaes[.]loginclienteb[.]mulasfer[.]leitungsen[.]de
- personal[.]bbvaes[.]loginclienteb[.]numerkilas[.]leitungsen[.]de
- personal[.]bbvaes[.]loginclienteb[.]tacuriols[.]lebtimnetz[.]de

Sample Malicious Properties Flagged during the Malware Check Dated 18 July 2022

- 2fa-app[.]info
- 2fa-app[.]buzz
- 2fa-app2[.]com
- wvvvv-app2fa[.]com
- secure-2fa[.]eu
- secure2fa[.]link
- secure-2fa-auth[.]com
- securedwells2fargo[.]com
- secure-app[.]xyz
- secureapp[.]shop
- app-2secure[.]com
- app-1secure[.]com
- secure-meapp[.]xyz
- td-secureapp[.]net
- applesecured01[.]com
- appsecureguide[.]com
- app-nodesecure[.]com
- secureds-review[.]app
- mycommsec-secure[.]app
- login-secure-app[.]com
- secureonline-app[.]com
- appdigitalsecure[.]com
- secure-app-de[.]online
- wells-secure01app[.]com
- barclays-secureapp[.]com
- mail[.]netflix-2fa-security-secureserver[.]misecure[.]com
- secureappsync[.]rf[.]gd
- appsecurechase[.]duckdns[.]org
- applesecured24[.]ddns[.]net
- secure062applid[.]duckdns[.]org
- appssecuremachas[.]onthewifi[.]com
- secured-app-i5m69[.]ondigitalocean[.]app
- www[.]secureappsync[.]rf[.]gd
- secure[.]diamica[.]app[.]antorislam[.]com
- secure[.]diamica[.]app[.]capitalprofit[.]online
- appsecureIncikchase[.]onthewifi[.]com
- secureserviceappers[.]merseine[.]com
- www[.]secure062applid[.]duckdns[.]org
- securepayment-apple[.]serveirc[.]com
- secure05-chasappsid[.]duckdns[.]org
- mail[.]secure062applid[.]duckdns[.]org
- app[.]greenlife-secure[.]bk-llc[.]info
- appsecurecitizens8531[.]duckdns[.]org
- myappbtsecurebusiness[.]github[.]io

- secureapplllesmauseda[.]is-certified[.]com
- www[.]secure[.]diamica[.]app[.]capitalprofit[.]online
- cpanel[.]secure062applid[.]duckdns[.]org
- www[.]secure05-chasappsid[.]duckdns[.]org
- webdisk[.]secure062applid[.]duckdns[.]org
- webmail[.]secure062applid[.]duckdns[.]org