IoCリストをもとに調査を展開、Gigabud RATの脅威の規模を測定

目次

要旨

世界中の政府を標的にしたサイバー攻撃は、特に斬新ではありません。しかし、モバイルアプリを使った攻撃は、戦術として非常に新しいものです。Cybleの研究者が先般、政府機関のモバイルアプリを使用するタイ、フィリピンおよびペルーのユーザーに狙いを定めたGigabud RATの手口を報告しました。

Cybleの分析では、この脅威に関与した6つのマルウェアハッシュと4つのURLがセキュリティ侵害インジケーター（IoC）として特定されました。WhoisXML APIはそのURLを3つのドメイン名と1つのIPアドレスに分解して独自に調査を展開し、それらに関連するアーティファクトを連鎖的に見つけ出しました。発見したものは以下の通りです。

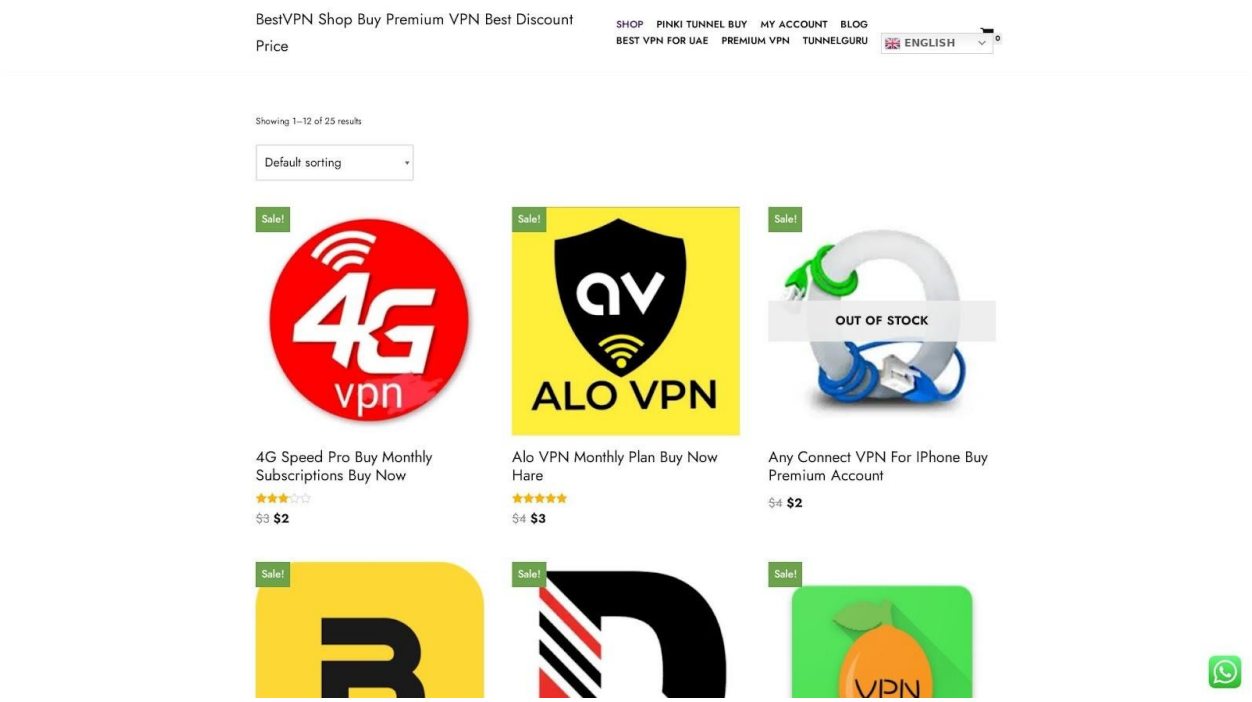
- IoCのドメイン名が名前解決した3つのIPアドレス
- 同じIPアドレスを使用していた301個のドメイン名。うち7つは悪意あるものと確認
- 共通の文字列を含む367個のドメイン名。そのうち8つはマルウェアホスト
- 共通のブランド名を含む519個のドメイン名。そのうち11個は悪意あるものと確認

Gigabud RATインフラの実態を解明

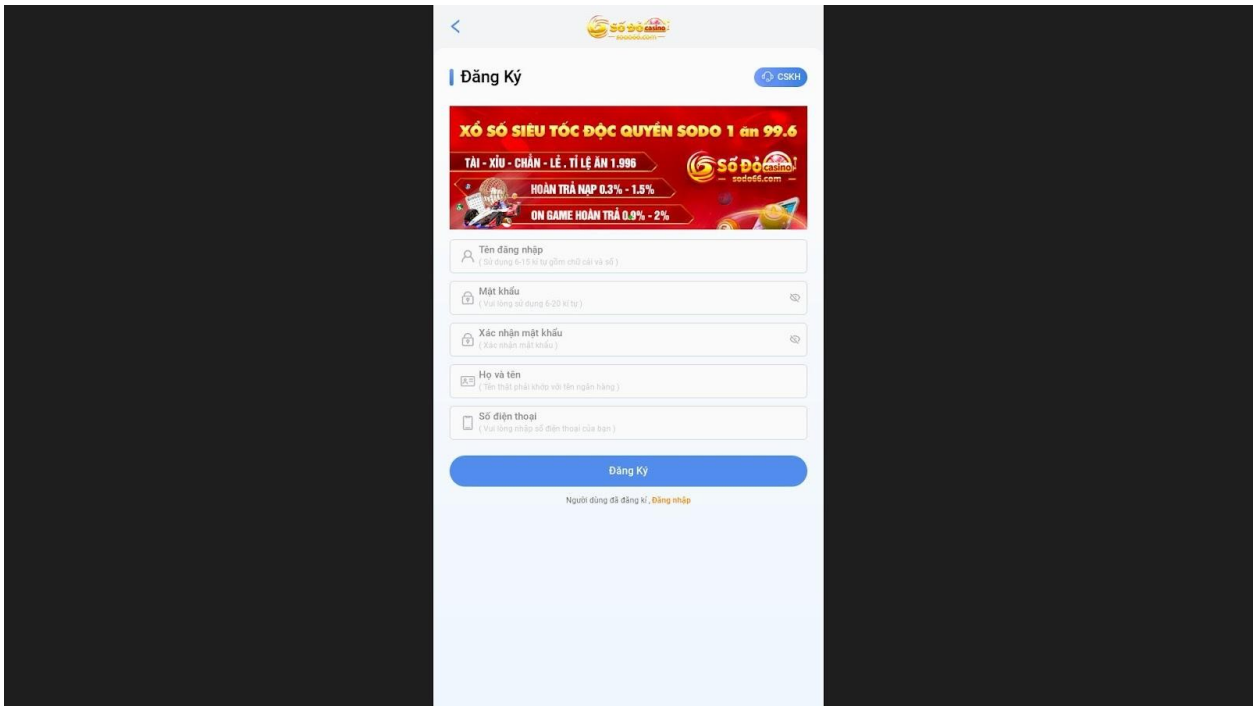
IoCと特定されたドメイン名をWHOIS lookupsで検索したところ、すべてのドメイン名の登録者が米国に所在していること、2022年11月から12月の間に新規登録されたことなど、興味深い共通点が見つかりました。ただ、cmnb9[.]ccというIoCは米国で登録された一方で、そのIPホストである18[.]143[.]123[.]20の地理的位置はシンガポールでした。

IoCとされたドメイン名をDNS lookupsで調べた結果、新たに3つのIPアドレス（18[.]143[.]123[.]20、104[.]21[.]41[.]159および172[.] 67[.]148[.]55）が判明しました。

これらのIPアドレスをキーワードとしてreverse IP/DNS lookup で検索したところ、IoCと同じIPアドレスを使っている301個のドメイン名を見つけました。これらのドメイン名はIoCと関連している可能性があります。それらについてマルウェアの一括チェックにかけたところ、7つが悪意あるドメイン名であることが確認されました。そして、screenshot lookupsでの検索により、live-bestvpnshop[.]com（VPNサービスを販売するショップのようです）とbrandmybooks[.]com（オンライン賭博サイトのようです）の2つは明らかに避けるべきものであることがわかりました。



bestvpnshop[.]comのスクリーンショット



brandmybooks[.]comのスクリーンショット

Gigabud RATのデジタルブレッドクラムをさらに探すために、IoCに見られるユニークな文字列をキーワードとしてDomains & Subdomains Discoveryで検索しました（下表の通り）。

IoC	検索ワードとして使用した文字列
• lionaiothai[.]com • cmnb9[.]cc • bweri6[.]cc	• ***lionaiothai.*** • ***cmnb*.*** • ***bweri*.***

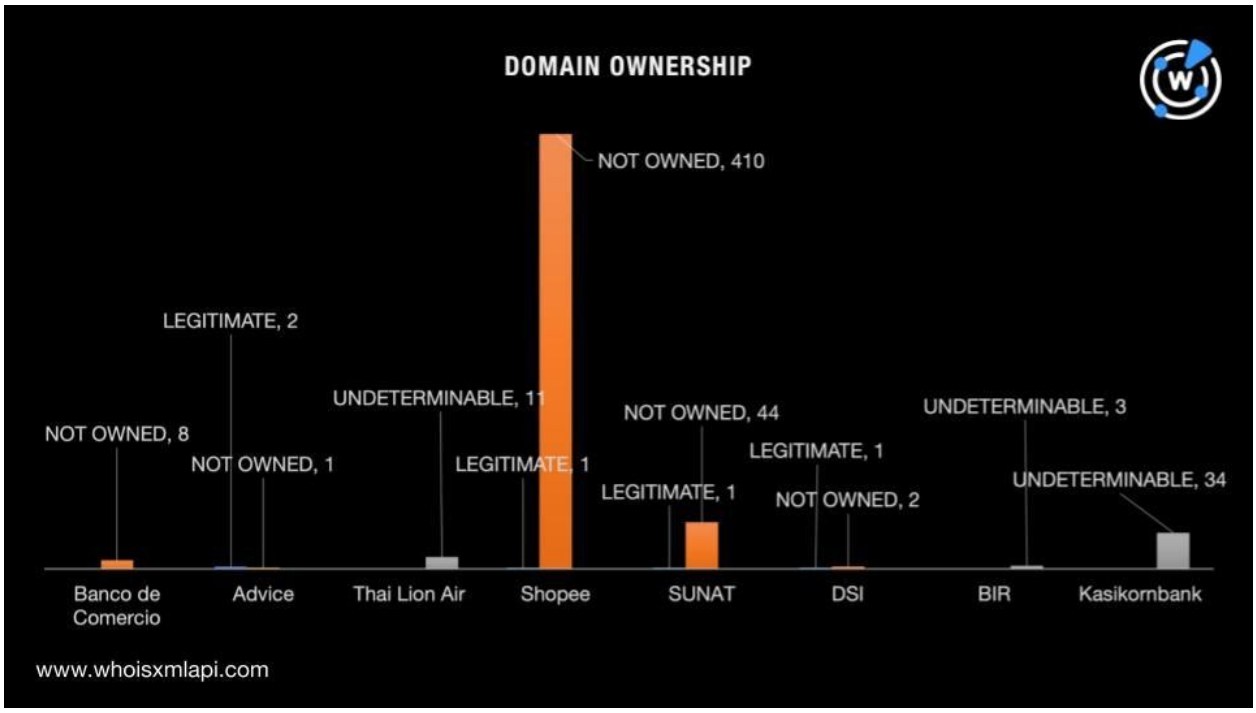
その結果、367個のドメイン名が見つかり、そのうち8つはマルウェアのホストと確認されました。これらのドメイン名は、ブロックリストに含めることが推奨されます。

Gigabud RATの分析では、Banco de Comercio、Advice、Thai Lion Air、Shopee、SUNAT、DSI、BIR、Kasikornbankも標的として挙げられていました。これらの組織名をDomains & Subdomains Discoveryの検索条件（使用した文字列は下表の通り）として使用することで、さらに519個のドメイン名を発見できました。そのうち11個は、マルウェアのホストでした。なお、検索対象は、単一の文字列で始まるもの、および1番目の用語で始まり2番目の用語を含む文字列の組み合わせに限定しました。

標的にされた組織	検索ワードとして使用した文字列

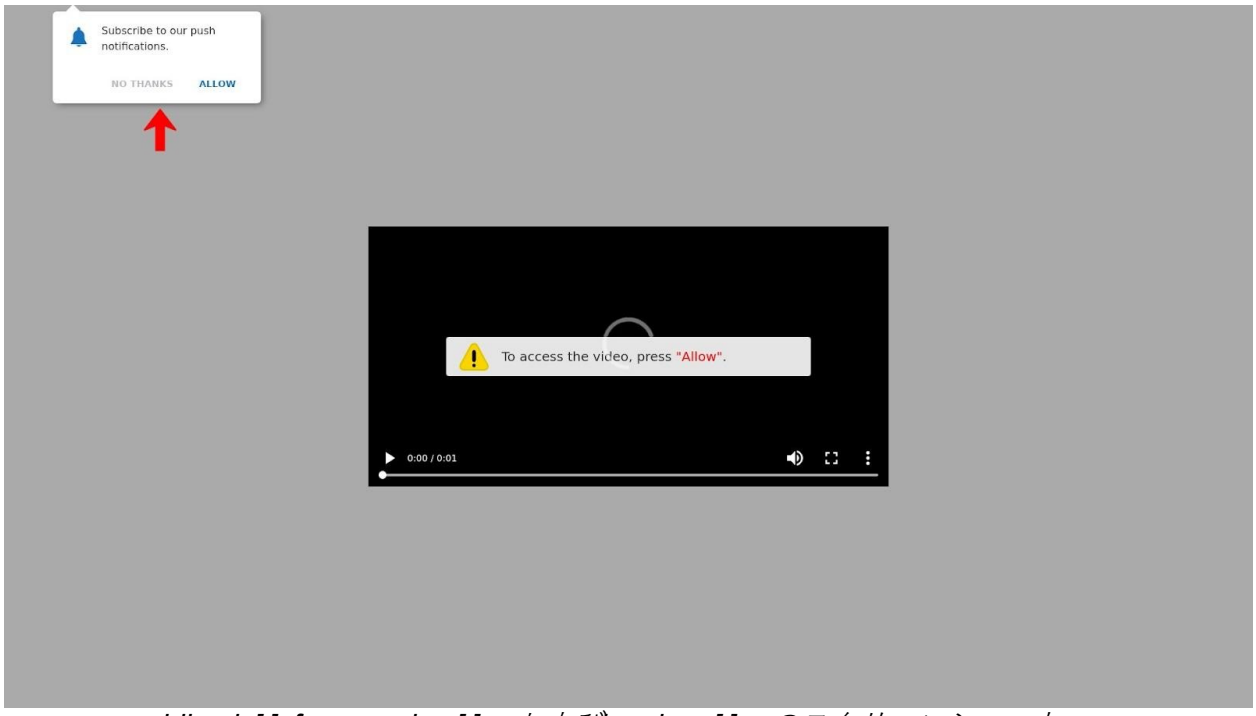
• Banco de Comercio • Advice • Thai Lion Air • Shopee Thailand • SUNAT • DSI (Department of Special Investigation Thailand) • BIR (Bureau of Internal Revenue Philippines) • Kasikornbank	• ***bancomercio.*** • ***advice.*** + ***th*** • ***lionairthai.*** • ***shopee.*** • ***sunat.*** • ***dsi.*** + ***th*** • ***bir.*** + ***ph*** • ***kasikornbank.***

正規のドメイン名とタイポスクワッティングの可能性があるドメイン名のWHOISレコードを比較したところ、519個のドメイン名のうち、文字列に名称が含まれた組織が実際に所有していたのはわずか5個、1%未満でした。ただし、Thai Lion Air、BIRおよびKasikornbankのドメイン名については、WHOISレコードが一部非表示にされていたため、正当性を確認できませんでした。



IPアドレス、文字列またはブランド名が共通しているすべてのドメイン名についてスクリーンショットを調べたところ、217個のドメイン名は今もアクセス可能で、有効なコンテンツをホストしていることがわかりました。エラーページ、インデックスページ、空白ページ、ドメイン名が現在販売中、工事中または修理中と表示されているページは除外しました。ゲーム、アダルトコンテンツ、チュートリアルサービスプロバイダー、ショッピング、ビジネスのサイトと思われるものもありました。IoCとの結びつきを考えると、不審な活動や侵害の兆候がないか監視する価値はありそうです。

少なくとも3つのウェブサイトは、ユーザーがコーデックをダウンロードしなければ再生されないビデオをホストしている（これはサイバー犯罪者がマルウェアを広めるために試行錯誤の末に生み出した手口です）ため、ブロックリストに含める必要があると思われます。



aldbzuic[.]cf、 aqyrobcs[.]gqおよびbezrkure[.]gaのスクリーンショット

bancomercio[.credit]という機関を模倣していると思われる以下のようなサイトも、ブロックする必要があります。

bancomercio[.]creditのスクリーンショット

—

Gigabud RATの4つのIoC（3つのドメイン名と1つのIPアドレス）をもとに今回行った調査では、マルウェアのホストとして確認された26個を含む、この脅威に関連するかもしれない未公開のアーティファクトが新たに1,190個発見されました。組織や個人、特に標的にされた機関の顧客は、見た目が似ているドメイン名や関連性のあるウェブプロパティをクリックしないように注意する必要があります。これらはすべて、銀行の認証情報を盗み出し、その画面の内容を記録するGigabud RATのソースとなる可能性があります。

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わせください。

付録：アーティファクトとIoCの例

Cybleが特定したIoC

- lionaiothai[.]com
- cmnb9[.]cc
- bweri6[.]cc
- 8[.]219[.]85[.]91

IoCとされたドメイン名が解決したIPアドレスの例

- 18[.]143[.]123[.]20
- 104[.]21[.]41[.]159

IoCのIPアドレスを共用していたドメイン名の例

- 123mkv[.]top
- 1billclub88[.]com
- 1vx0lvodabe4bf[.]fun
- 2xsvb1a[.]shop
- 36sag6[.]com
- 3lancer[.]io
- 479fire[.]org
- 500dresses[.]org
- 5219q[.]com
- 5bbprofit[.]shop
- 6gmmdv[.]net
- 77663885[.]com
- 778charlie[.]com
- 91mw[.]net
- 9519265[.]com
- a-great-criminal-justice-yg[.]fyi
- a1freegames[.]com
- aackj6[.]cc
- aackj7[.]cc
- aarmi[.]org
- abatic[.]ca
- abokcakingau[.]tk
- acalrimrirar[.]ga
- acc311[.]com
- acgemidisanar[.]ml
- ackneecesrodce[.]tk
- acmc-corrosion[.]com
- actigarconog[.]tk
- adelabel[.]com
- admiredwattdistr[.]top
- adrilpart[.]cf
- adxhype[.]com
- africatime[.]com
- agenartersauflor[.]tk
- ahenectheacase[.]cf
- aidingtheenemy[.]com
- aips[.]gr
- ajogaron[.]dplus[.]org
- akbar-marble[.]com
- aknoo[.]com
- alapictos[.]ml
- albanygate[.]com
- aldbzuic[.]cf
- alentatgio[.]tk
- alkhabbazsa[.]com
- allefree[.]co
- alwide[.]ga
- amcomcatalscepma[.]ga
- americanfleetautoservice[.]com
- amisucisunnes[.]cf

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

- 123mkv[.]top
- bagi2diamongratis[.]baruup2022[.]cf
- baruup2022[.]cf
- bestvpnshop[.]com

IoCに見られる文字列を含んだドメイン名の例

- lionaiothai[.]cc
- cmnbrazil[.]org
- cmnb[.]vip
- cmnba[.]com
- cmnbdrz[.]cn
- cmnby[.]loan
- cmnbe[.]com
- cmnbns[.]info
- cmnbmn[.]gq
- cmnb10pnq[.]nom[.]za
- cmnbui[.]ga
- cmnbp[.]com
- cmnb5stepprocess[.]net
- cmnbpro[.]com
- cmnb[.]xin
- cmnb07[.]cn
- cmnbt[.]link
- cmnbgg[.]com
- cmnbisystore[.]com
- cmnbr[.]com
- cmnbhrsf[.]cn
- cmnbvcbxvxcxbbmn[.]net
- cmnb[.]icu
- cmnbjt[.]wang
- cmnbilingualschool[.]com
- cmnbf[.]top
- cmnbs[.]loan
- cmnbainsight[.]com
- cmnbb[.]tk
- cmnbgh[.]top
- cmnbui[.]ml
- cmnb7ke[.]cyou
- cmnbdz[.]cn
- cmnb5stepprocess[.]biz
- cmnbewr[.]info
- cmnb92[.]ltd
- cmnbz6e92o[.]biz
- cmnbrands[.]network
- cmnbj[.]loan
- cmnbnvamaygmlfxsdisuozpvwot[.]biz
- cmnbgr[.]top
- cmnbgp[.]top
- cmnbahi[.]info
- cmnbid[.]com
- cmnbj[.]com
- cmnbg[.]loan
- cmnb5stepprocess[.]org
- cmnbfk[.]top
- cmnbrands[.]com[.]my
- cmnb[.]co[.]kr

共通の文字列を含む悪意あるドメイン名の例

- cmnbmo[.]cf
- cmnbmo[.]gq
- cmnbpp95[.]icu
- cmnbv[.]bid

標的にされた組織のブランド名を含むドメイン名の例

- bancomercio[.]es
- bancomercio[.]com[.]pe
- bancomercio[.]site
- bancomercio[.]info
- bancomercio[.]com
- bancomercio[.]pe
- bancomercio[.]com[.]br
- bancomercio[.]credit
- bancomercio[.]net
- advice[.]th
- advice[.]co[.]th
- advice[.]in[.]th
- lionairthai[.]in
- lionairthai[.]com[.]tw

- lionairthai[.]com
- lionairthai[.]co[.]uk
- lionairthai[.]net
- lionairthai[.]co[.]in
- lionairthai[.]com[.]vn
- lionairthai[.]cn
- lionairthai[.]co
- lionairthai[.]tw
- lionairthai[.]com[.]cn
- shopee[.]xn--6qq986b3xl
- shopee[.]com[.]bz
- shopee[.]wine
- shopee[.]ooo
- shopee[.]ac[.]cn
- shopee[.]family
- shopee[.]space
- shopee[.]co[.]za
- shopee[.]cheap
- shopee[.]tv
- shopee[.]house
- shopee[.]ind[.]in
- shopee[.]to
- shopee[.]world
- shopee[.]poker
- shopee[.]bio
- shopee[.]kz
- shopee[.]shopping
- shopee[.]ke
- shopee[.]mv
- shopee[.]gift
- shopee[.]tools
- shopee[.]org[.]pl
- shopee[.]mobi
- shopee[.]town
- shopee[.]nu
- xn--shop-jpa9v[.]ph
- shopee[.]golf
- shopee[.]me
- shopee[.]so
- shopee[.]party
- shopee[.]one
- shopee[.]delivery
- shopee[.]love
- shopee[.]nom[.]za
- shopee[.]app
- shopee[.]express
- shopee[.]gifts
- shopee[.]net[.]ph
- shopee[.]xn--3ds443g
- shopee[.]capital
- shopee[.]beauty
- shopee[.]ren
- shopee[.]com[.]pt
- shopee[.]wang
- shopee[.]ltd
- shopee[.]life
- xn--shope-7ra[.]com
- shopee[.]shop[.]pl
- shopee[.]kiwi
- xn--hop-uraa50b[.]ph
- shopee[.]cards
- shopee[.]gdn
- shopee[.]bz
- shopee[.]rip
- shopee[.]kim
- shopee[.]rs
- shopee[.]marketing
- shopee[.]discount
- shopee[.]re
- shopee[.]lol
- shopee[.]net
- shopee[.]ml
- shopee[.]chat
- shopee[.]monster
- shopee[.]city
- shopee[.]green
- shopee[.]supply
- shopee[.]info[.]vn
- shopee[.]immo
- shopee[.]mk

- shopee[.]luxury
- shopee[.]engineer
- shopee[.]eu
- shopee[.]audio
- shopee[.]jewelry
- shopee[.]events

共通のブランド名を含む悪意あるドメイン名の例

- shopee[.]party
- shopee[.]gq
- shopee[.]ga
- shopee[.]ee
- xn--shpee-1ta[.]vn
- shopee[.]moda