ユーザーを騙してダウンロードさせるSocGholishのIoCとアーティファクト

目次

要旨

初期アクセス型の脅威の中でも、SocGholishは最も厄介なものの一つです。SocGholishの手口は、ソフトウェアの更新を装ってユーザーに悪意あるペイロードをダウンロードさせ、そこから致命的なサイバー攻撃へと発展させるというものです。先般、ReliaQuestにより、SocGholishマルウェアの配布がランサムウェアの展開を意図したものであった証拠が明らかになりました。

ReliaQuestはまた、コマンド＆コントロール（C&C）ドメインとIPアドレスという形で、6つのセキュリティ侵害インジケーター（IoC）を挙げました。これを受け、当社はドメイン名、IPアドレス、DNSのインテリジェンスを駆使し、IoCの足跡を追ってみました。その結果、次のことがわかりました。

- 脅威アクターは、悪意あるサブドメインをホストするために、古いルートドメインや最近登録されたルートドメインを使用
- 1個のIoCの登録者メールアドレスから、200以上の関連したドメイン名が判明
- それらのドメイン名のうち5%超は悪意あるドメイン名で、その多くが***update***という文字列を含む
- 共通のネームサーバーや文字列の使用を手掛かりに、IoCと関連した数十個のアーティファクトがさらに判明

SocGholishのIoCについてわかっていること

ReliaQuestは、SocGholishの活動に関連しているIoCとして以下を特定しました。

- taxes[.]rpacx[.]com
- *.signing[.]unitynotarypublic[.]com
- *.asset[.]tradingvein[.]xyz
- 88[.]119[.]169[.]108
- change-land[.]com
- 31[.]184[.]254[.]115

上記のIoCはSocGholishとCobalt StrikeのC&Cサーバーを組み合わせたもので、脅威アクターは後者を侵入後の活動に使用していました。これらのウェブプロパティは、同一の悪意あるアクターに結びついていた可能性があります。

これらのIoC（IoCとされたサブドメインのルートドメインを含む）をhistorical WHOIS dataで検索したところ、以下が明らかになりました。

IoC	ルートドメインの新規登録日	レジストラ	登録者
taxes[.]rpacx[.]com	2009年3月10日	FastDomain Inc.	2019年よりプライバシー保護のため非公開。過去に公開されていたメールアドレスが、現在別のドメイン名1個と関連している
*.signing[.]unitynotarypublic[.]com	2021年9月29日	Launchpad.com Inc.	ドメイン名新規登録以降プライバシー保護のため非公開
*.asset[.]tradingvein[.]xyz	2022年12月22日	Namecheap	ドメイン名新規登録以降プライバシー保護のため非公開
change-land[.]com	2022年1月26日	REG.RU LLC	218個のドメイン名と関連している1つの公開メールアドレスとともに、未編集のまま公開

サブドメインのコントロール方法にかかわらず、脅威アクターは古いドメイン名と最近登録されたドメイン名を組み合わせてC&Cサーバーに使用していました。

IoCとされたIPアドレスをIP Geolocation APIで調査した結果は、以下のようになりました。

IoC	IPアドレスの地理的位置	ISP	名前解決の状態
88[.]119[.]169[.]108	リトアニア・シャウレイ群	Informacines Sistemos Ir Technologijos, UAB	名前解決しない、またはドメイン名との関連なし
31[.]184[.]254[.]115	ロシア・サンクトペテルブルク	Selectel	1個のドメイン名（change-land[.]com）と関連

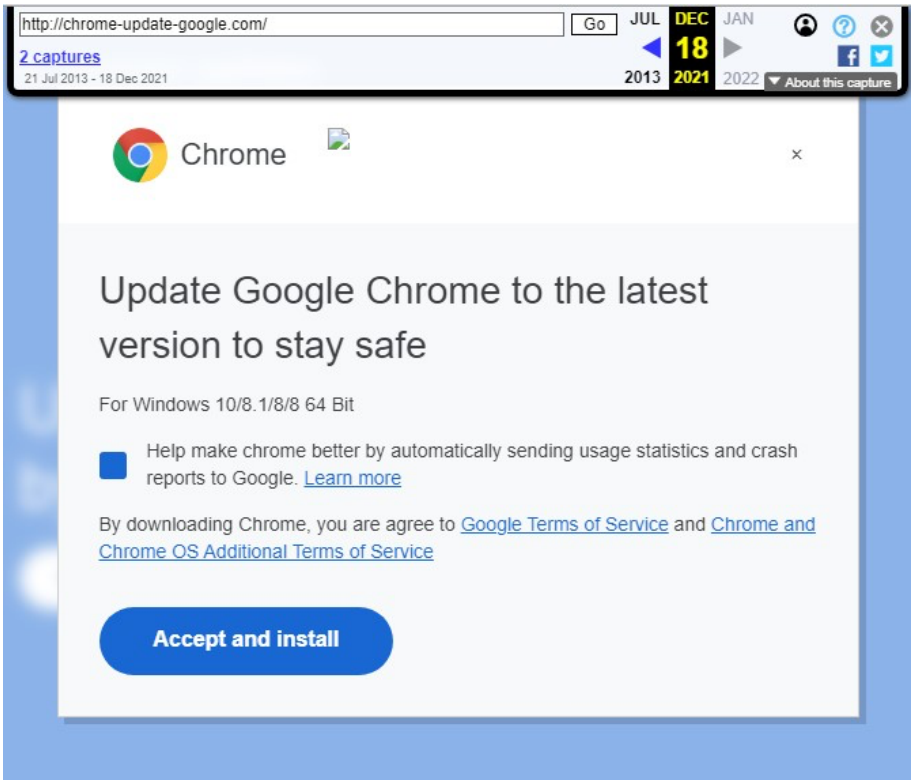
SocGholishのIoCから分析の範囲を拡大：メールアドレス、ネームサーバー、共通の文字列を追跡

上記のようにIoCのプロファイリングを行ったことで、追求するべきデータを決定できました。IoCをもとに行った以下の分析では、登録者の情報が公開されていたchange-land[.]comに焦点を当てました。

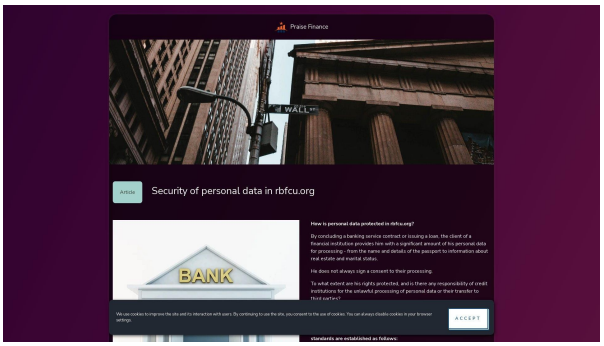
公開されている登録者のメールアドレスから足跡を追う

Reverse WHOIS Searchで検索したところ、change-land[.]comと同じ登録者メールアドレスをWHOISで表示していたドメイン名が218個見つかりました。それらのドメイン名のうち5%あまりは悪意あるものでした。

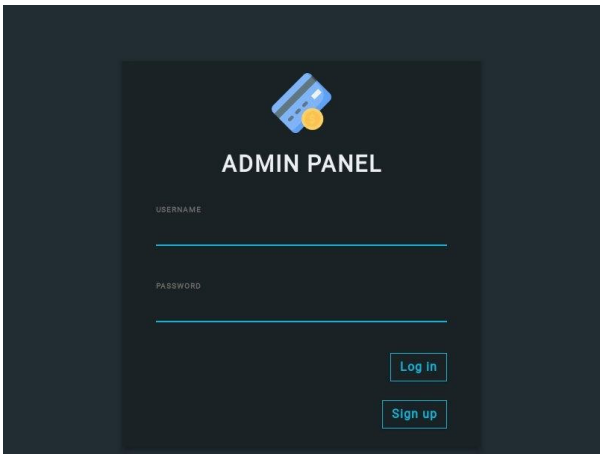
chrome-update-google[.]comがその一例です。現在は名前解決しないものの、2021年当時は以下のコンテンツをホストしていました。



この記事の執筆時点でも、関連性がある一部のドメイン名はコンテンツをホストし続けています。例えば、change-land[.]comと同じ登録者メールアドレスを共有する以下のドメイン名などです。

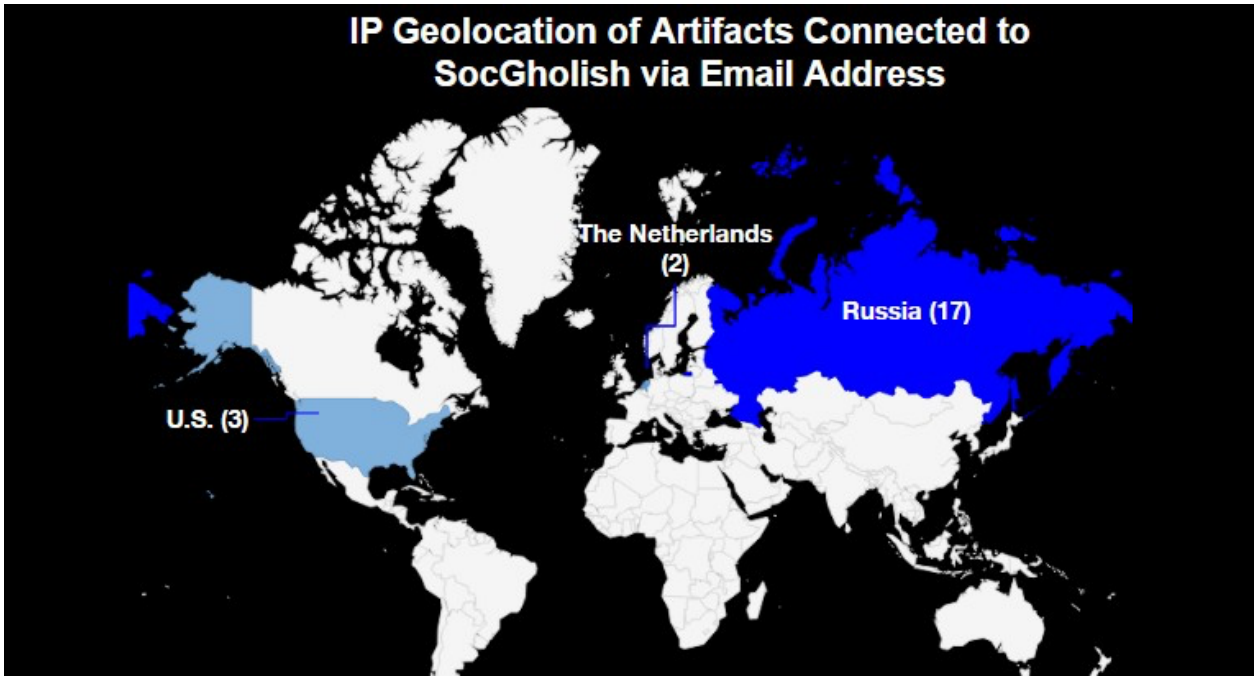


secretswab[.]netのスクリーンショット



sell-cvv[.]comのスクリーンショット

WHOISデータで関連性が見られる218個のドメイン名のうち、21個は18のユニークなIPアドレスに名前解決し続けていました。さらに、Bulk IP Geolocationにより、それらの大部分はC&Cサーバーの IPアドレスである31[.]184[.]254[.]115のように、ロシアに行き着く可能性があるとわかりました。



また、それらのアーティファクトのIPジオロケーションデータとIoCである31[.]184[.]254[.]115のジオロケーションデータの類似点として、ほとんどがISPとしてSelectelを採用していたことが挙げられます。

その他、Alibaba、Dolgova Alena Andreevna、Hosting Technology Ltd、Cloud Assets LLCといったISPが確認されています。

WHOISの繋がりをさらに掘り下げる

IoCとアーティファクトの間にIPジオロケーションとISPの点で類似性があることから、さらにそのドメインインフラを調査することにしました。

WHOISデータに共通点があるアーティファクトをbulk WHOIS lookupで調べたところ、ほぼすべてのドメイン名がa.dnspod[.]com|c[.]dnspod[.]comというネームサーバーを使っていることがわかりました。また、ほとんどのドメイン名のレジストラがREG.RU LLC.でした。

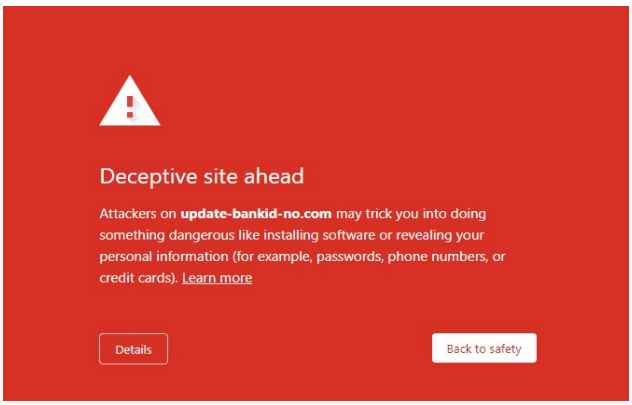
これらのWHOISデータを検索文字列としてReverse WHOIS Searchにかけた結果、2023年1月1日から2月22日の間に新規登録されたものを含む、潜在的な関連ドメイン名がさらに見つかりました。具体的には、Slack、Evri、Bank of Americaおよび仮想通貨のウォレットであるTrezorを標的としたタイポスクワッティングドメインを含む、34個のドメイン名が特定されました。

さらに、それらをマルウェアチェックにかけたところ、最近登録されたドメイン名のうち数件がすでに悪意あるキャンペーンに利用されていたことがわかりました。

共通の文字列を含む新規登録ドメイン名

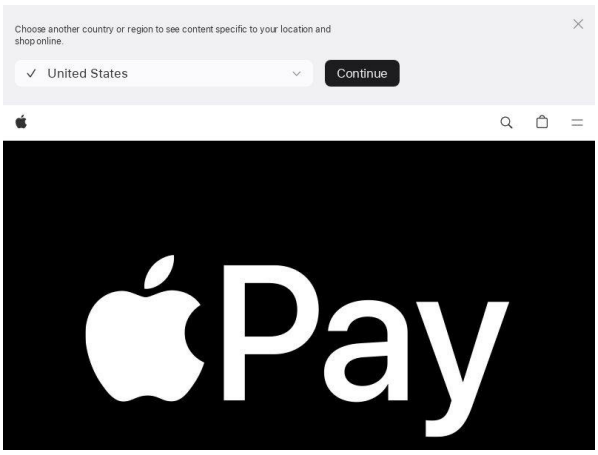
悪意あるドメイン名のほとんどは、***update***、***bank***、***wallet***および***Google***といった文字列を含んでいました。これらの文字列の組み合わせを持つドメイン名をさらに見つけるために、Domains & Subdomains Discoveryを使って2023年1月1日から2月22日の間に新規登録されたドメイン名に限定して検索してみました。

その結果27個のドメイン名が新たに見つかり、半数あまりが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。以下はその例です。



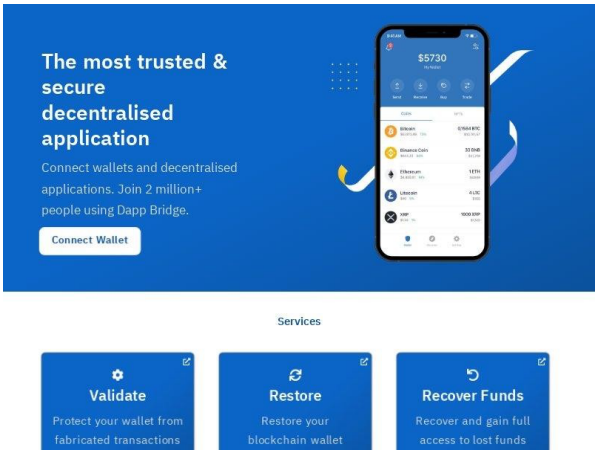
*update-bankid-no[.]com*のスクリーンショット

*commbank-update-au[.]com*のスクリーンショット

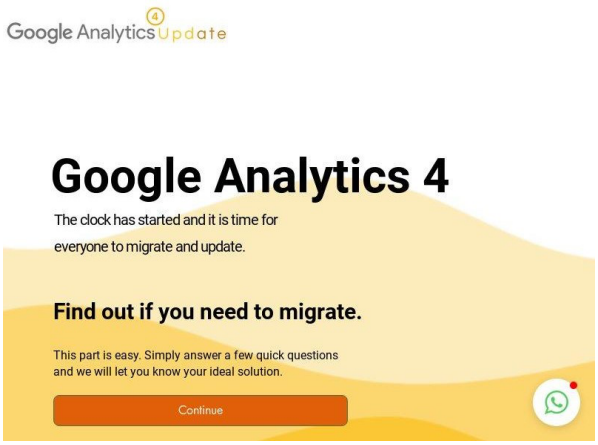


myapplewallet-update[.]comの
スクリーンショット

googledailyupdaterepo[.]comの
スクリーンショット



dappwallet-update[.]comの
スクリーンショット



googleanalyticsupdate[.]comの
スクリーンショット

なお、update-bankid-no[.]comとcommbank-update-au[.]comは、文字列に共通点があり最近登録された他の4つドメイン名とともに、既に悪意あるものとして報告されています。

—

SocGholishのIoCを出発点として、IPジオロケーション、ISP、ネームサーバー、レジストラおよびドメイン名に含まれる文字列のパターンを調査した結果、さらに何百もの疑わしいドメイン名が見つかりました。そして、その一部はSocGholishと同じ偽の更新という手口を使っていることもわかりました。

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

IoCの背後にある同一の存在によって登録されたドメイン名の例

- rdrcmtiscl[.]com
- riattivare-tiscali-mail[.]com
- login-tiscali-mail[.]com
- rdrctiscl[.]com
- riativare-tiscali-mail[.]com
- change-land[.]com
- expresswayprojects[.]com
- combustiblescolombia[.]com
- lunaswab[.]com
- luckylunacrybto[.]com
- dsgmetavers[.]com
- pocket-lingo[.]com
- medicare-cost[.]com
- intradayinvestment[.]com
- marktplaatsverificatieupdate[.]com
- mad-colour[.]com
- boi365mobileapplication[.]com
- pastorcryptograph[.]at
- secretswab[.]net
- electronic-infinity[.]com
- crossswab[.]com
- crosswab[.]com
- edrop[.]su
- bambooreley[.]com
- musliswap[.]com
- stellartem[.]com
- shabeshift[.]com
- sundaeswab[.]com
- muesliswab[.]com
- bancosantanderacess[.]com
- bancosantanderacesso[.]com
- thorswab[.]com
- olongswab[.]com
- rocetpool[.]net
- roketpool[.]net
- runinchain[.]com
- deversifiy[.]com
- eterdelta[.]com
- oolongswab[.]com
- sunswab[.]com
- dgsmetavers[.]com
- dsgmetaver[.]com
- assetsclick[.]com
- swipestore[.]su
- xdaichan[.]com
- deverifi[.]com
- sweetdog[.]net
- lovelcat[.]net
- era-production[.]com
- simsmssender[.]com

IoCと同じネームサーバーを使用し共通の文字列を含む、2023年1月1日から2月22日までの間に登録されたドメイン名の例

- 5lack[.]net
- bankid-app[.]com
- rufus-ie[.]net
- delta-communitycu[.]com
- targos-identification-kq983498[.]com
- dkb-entry-wp983948[.]com
- ml-bofa[.]com
- dickpicpost[.]com
- book-redelivery[.]com
- meine-santandern-entry-dp087837487[.]com
- energy-rebatescheme-gb[.]com
- boredape-yacht-club[.]com

- oredape-yacht-club[.]com
- www-bayc[.]com
- trrezer[.]net
- trrezor[.]net
- trezzer[.]net
- trezoor[.]net
- evri-delivery-attempt[.]com
- actions-bendigo[.]com
- googleupdateviewer[.]com
- googlebetterupdates[.]com
- googleanalyticsupdate[.]com
- googledailyupdaterepo[.]com
- googlesecurityupdates[.]com
- google-code-updates[.]msk[.]ru
- updatewallets[.]io
- dappwallet-update[.]com
- update-trustwallets[.]com
- updatewallet-client[.]com
- wallet-update-ports[.]com
- myapplewallet-update[.]com
- applewallet-update3782[.]com
- dzbankupdates[.]com
- banksupdate[.]email
- l-bank-update[.]xyz
- update-bankid-no[.]com
- commbank-update-au[.]com
- acces-updatesibank[.]com
- updateaddressusbank[.]com

2023年2月22日時点で悪意があると確認されているドメイン名の例

- login-tiscali-mail[.]com
- secretswab[.]net
- bancosantanderacess[.]com
- bancosantanderacesso[.]com
- 0-update[.]com
- sky-bill[.]com
- makemoneyonlinefrom-home[.]com
- icontraininginstitute[.]com
- rubbershot[.]com
- orangebronze[.]com
- jqueryllc[.]net
- redirect-customer01[.]com
- voting-xrp[.]net
- redirect-customer2[.]com
- www-stepn[.]com
- azureinput[.]com
- amexpressservice[.]com
- wwv-hex[.]com
- op743hfe6y34bsdsbxsvnnreyre[.]xyz
- ritvrlbml[.]com
- riattivare-servizio-libero-mail[.]com
- meamaskwalletupdate[.]com
- pancakswap[.]at
- dao-mahker[.]com
- htaminorfault[.]xyz
- daymong[.]xyz
- combankupdate[.]com
- boimobappp[.]com