SocGholish IoCs and Artifacts: Tricking Users to Download Malware

Table of Contents

Executive Report

As all initial-access threats go, SocGholish is among the trickiest. It often comes disguised as software updates, deceiving victims into downloading a malicious payload that could eventually lead to more lethal cyber attacks. In fact, researchers at ReliaQuest found evidence that an initial SocGholish malware distribution was intended to deploy ransomware.

The researchers also listed six indicators of compromise (IoCs) in the form of command-and-control (C&C) domains and IP addresses. We mapped the footprints of these IoCs using domain, IP, and DNS intelligence and found that:

- The threat actors used old and recently registered root domains to host malicious subdomains.
- One IoC's unredacted registrant email address led us to 200+ connected domains.
- More than 5% of these artifacts were malicious, with many containing the string ***update***.
- Dozens of additional artifacts were found related to the IoCs, either through name server or string usage.

What We Know about the SocGholish IoCs

ReliaQuest listed the following properties as IoCs involved in the SocGholish distribution activities they detected:

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

These IoCs combined SocGholish and Cobalt Strike C&C servers since threat actors used the latter for post-exploitation. At any rate, these web properties could still be tied to the same malicious actor.

The historical WHOIS data of these digital resources, including the root domains of the subdomains tagged as IoCs, revealed the following:

IoC	Creation Date of the Root Domain	Registrar	Registrant
taxes[.]rpacx[.]com	10 March 2009	FastDomain Inc.	Redacted for privacy since 2019, with one historical public email address currently connected to one domain
*.signing[.]unitynotary public[.]com	29 September 2021	Launchpad.com Inc.	Redacted for privacy since its creation
*.asset[.]tradingvein[.]xyz	22 December 2022	Namecheap	Redacted for privacy since its creation
change-land[.]com	26 January 2022	REG.RU LLC	Unredacted, with one public email address currently connected to 218 domains

Regardless of the method by which the threat actors controlled the subdomains, they used a combination of old and recently registered domains as C&C servers.

As for the IP addresses tagged as IoCs, these are their details based on IP Geolocation API:

IoC	IP Geolocation	ISP	Resolution Status
88[.]119[.]169[.]108	Šiauliai County, Lithuania	Informacines Sistemos Ir Technologijos, UAB	No resolutions or domain connections
31[.]184[.]254[.]115	Sankt-Peterburg, Russia	Selectel	Connected to one domain (change-land[.]com)

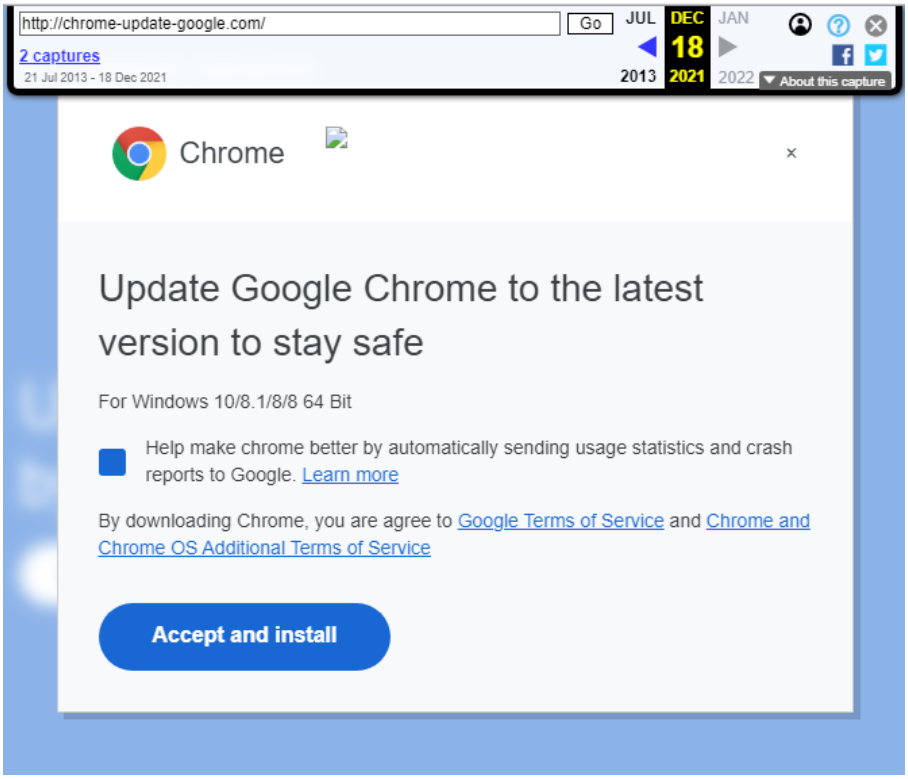
SocGholish IoC Expansion Analysis: Chasing an Email Address, Name Servers, and Recurring Strings

Profiling the IoCs in the previous section helped us determine which data points to pursue. We focused on change-land[.]com for the following IoC expansion analysis since its registrant details were publicly available.

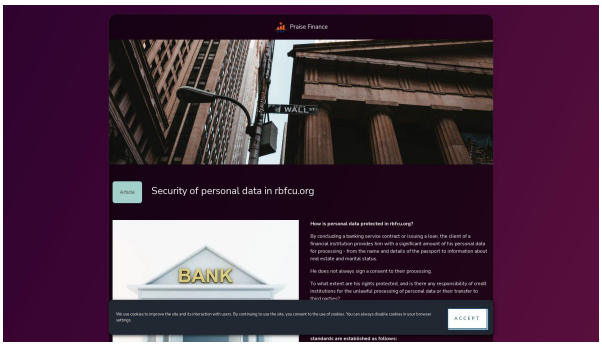
Tracing the Footprint of a Public Registrant Email Address

Using Reverse WHOIS Search, we found 218 domains sharing the same public registrant email address as change-land[.]com. More than 5% of these WHOIS-connected artifacts were malicious.

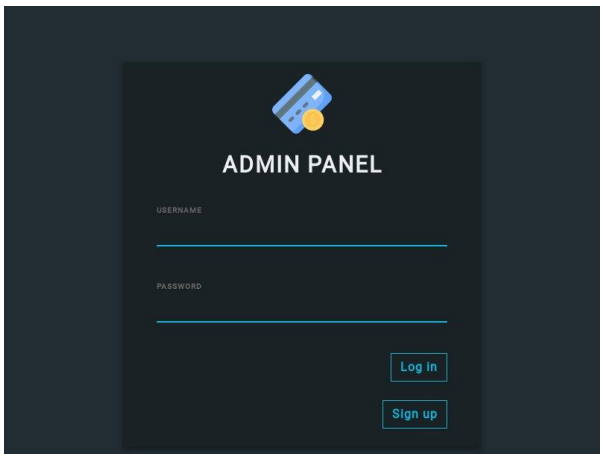
An example is chrome-update-google[.]com. Although it no longer resolves, the domain hosted the following content back in 2021:



Still, some connected domains continued to host content as of this writing. A few examples include these domains that also shared the same registrant email address as change-land[.]com:

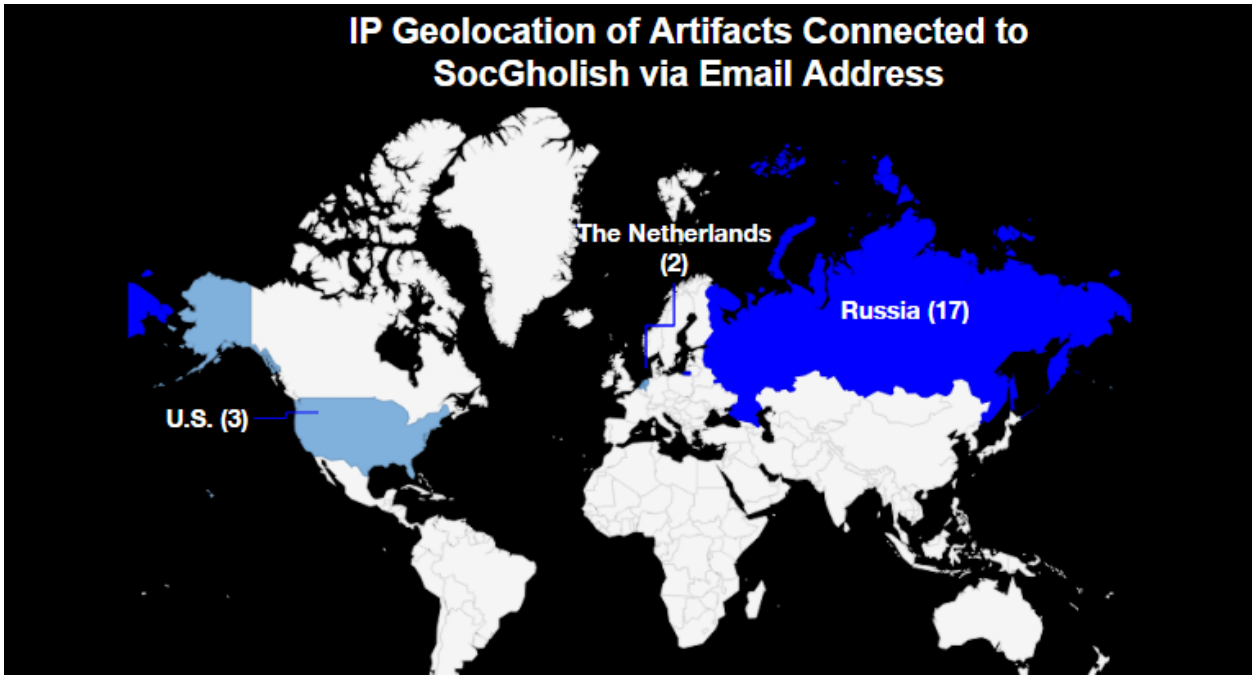


Screenshot of secretswab[.]net



Screenshot of sell-cvv[.]com

Of the 218 WHOIS-connected artifacts, 21 continued to actively resolve to 18 unique IP addresses. Bulk IP Geolocation further revealed that a majority of these resolutions could be traced to Russia, like the C&C server IP address 31[.]184[.]254[.]115.



Another similarity between the artifacts' IP geolocation data and that of IoC 31[.]184[.]254[.]115 was that most of them had Selectel as their ISP.

Other ISPs identified include Alibaba, Dolgova Alena Andreevna, Hosting Technology Ltd., and Cloud Assets LLC.

Digging for More WHOIS Connections

The similarities in IP geolocation and ISP among the IoCs and artifacts led us to examine their domain infrastructures to find more associations.

Subjecting the WHOIS-connected artifacts to a bulk WHOIS lookup allowed us to find that the registrant used the name server a.dnspod[.]com|c[.]dnspod[.]com for almost all the domains. Most of the domains' registrar was also REG.RU LLC.

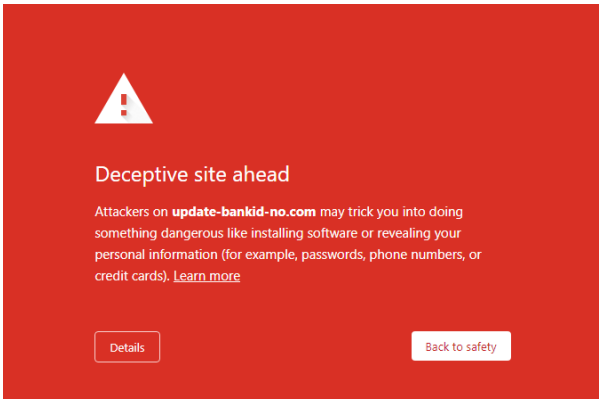
We used these WHOIS data points as search strings on Reverse WHOIS Search to retrieve more possible artifacts, specifically those created between 1 January and 22 February 2023. The tool returned 34 domains, including typosquatting properties targeting Slack, Evri, the Bank of America, and crypto wallet Trezor.

Moreover, a malware check on the properties revealed that a few of the recently registered domains had already figured in malicious campaigns.

Uncovering Recently Added String-Connected Artifacts

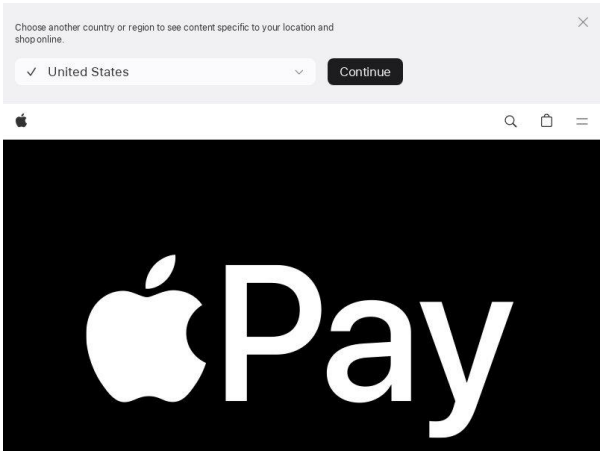
Most of the malicious artifacts we found contained the string ***update***, used alongside ***bank***, ***wallet***, and ***Google***. To find additional artifacts bearing these string combinations, we used Domains & Subdomains Discovery and limited our search to domains added between 1 January and 22 February 2023.

We found 27 domains, more than half of which hosted live content. Below are a few examples.



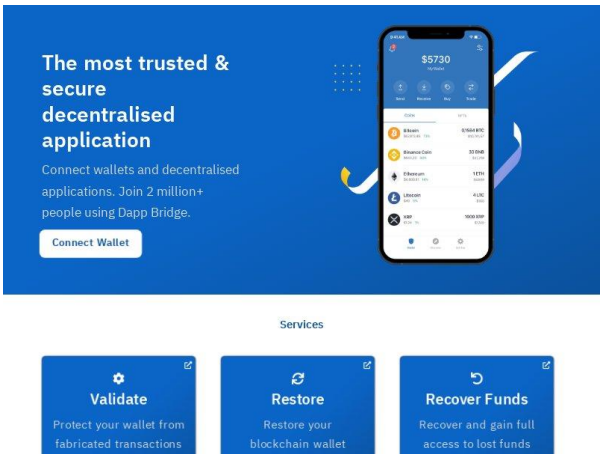
Screenshot of update-bankid-no[.]com

Screenshot of commbank-update-au[.]com

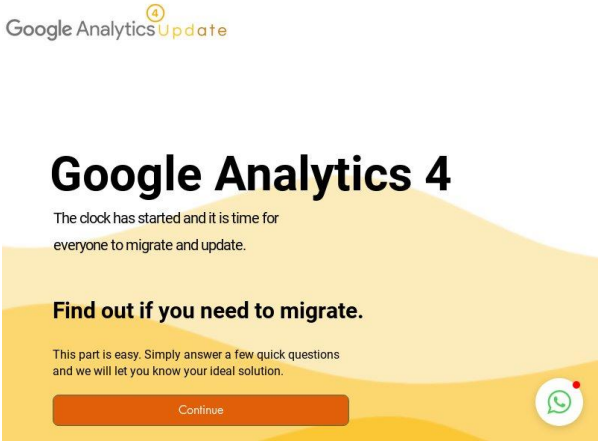


Screenshot of myapplewallet-update[.]com

Screenshot of googledailyupdaterepo[.]com



Screenshot of dappwallet-update[.]com



Screenshot of googleanalyticsupdate[.]com

Note that update-bankid-no[.]com and commbank-update-au[.]com have already been reported as malicious, along with four other recently registered string-connected artifacts.

—

One SocGholish IoC led us to hundreds of additional suspicious domains, some of which fit the bill of the threat's fake update tactic. We did that by looking for recurring patterns in their IP geolocations, ISPs, name servers, registrars, and text strings.

If you wish to perform a similar investigation or get access to the complete data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Domains Registered by the Same Entity behind an IoC

- 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

Sample Domains Sharing the IoCs' Name Servers and Recurring Strings Added from 1 January to 22 February 2023

- 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

Sample Malicious Domains Flagged as of 22 February 2023

- 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