WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

On the Hunt for Remnants of the Samourai Wallet Crypto Mixing Services in the DNS

Table of Contents

Executive Report

Keonne Rodriguez and William Lonergan Hill, founders of Samourai Wallet, a cryptocurrency mixing service, were sentenced in April 2024 and their sites taken down for executing more than US$2 billion in unlawful transactions and laundering more than US$100 million in criminal proceeds. Are all traces of the illegal business in the DNS gone? Or do some remain? The WhoisXML API research team sought to find out.

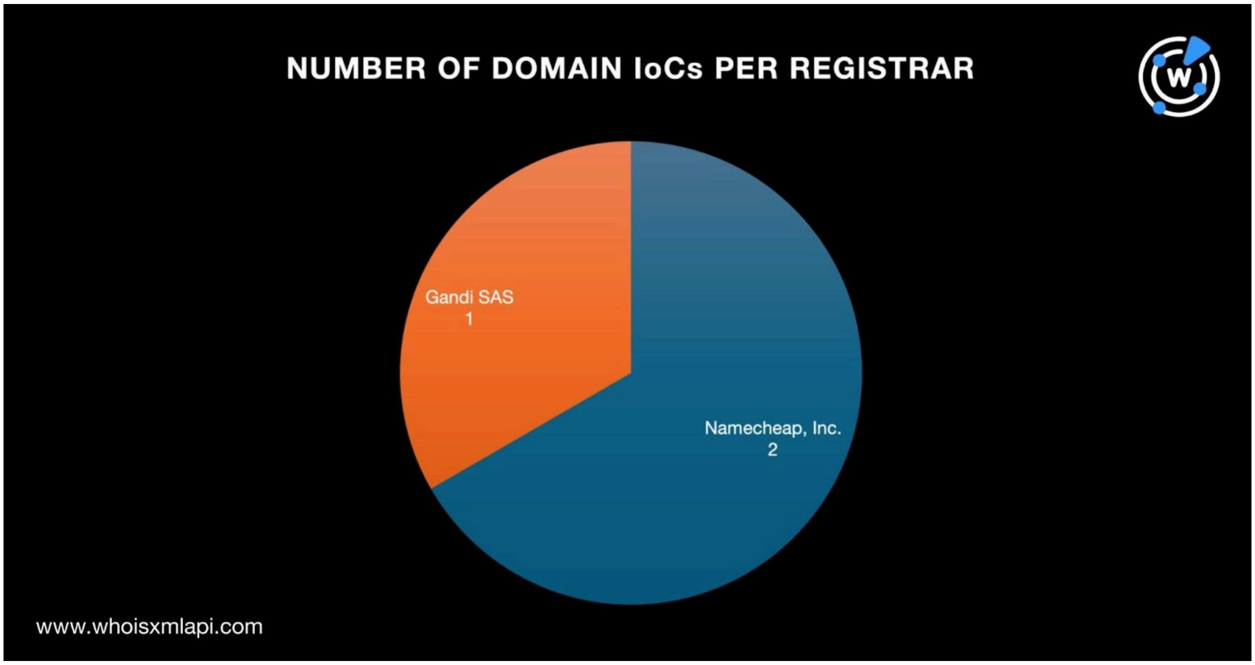
Our team obtained three domains tagged as Samourai Wallet indicators of compromise (IoCs)—samourai[.]io, samourai[.]support, and samouraiwallet[.]com—from threat researcher Dancho Danchev. To uncover possibly related threat artifacts that remain unidentified to date, we expanded the list of IoCs aided by our comprehensive DNS intelligence sources and found:

- Four IP addresses, three of which are malicious
- Two IP-connected domains
- 66 string-connected domains

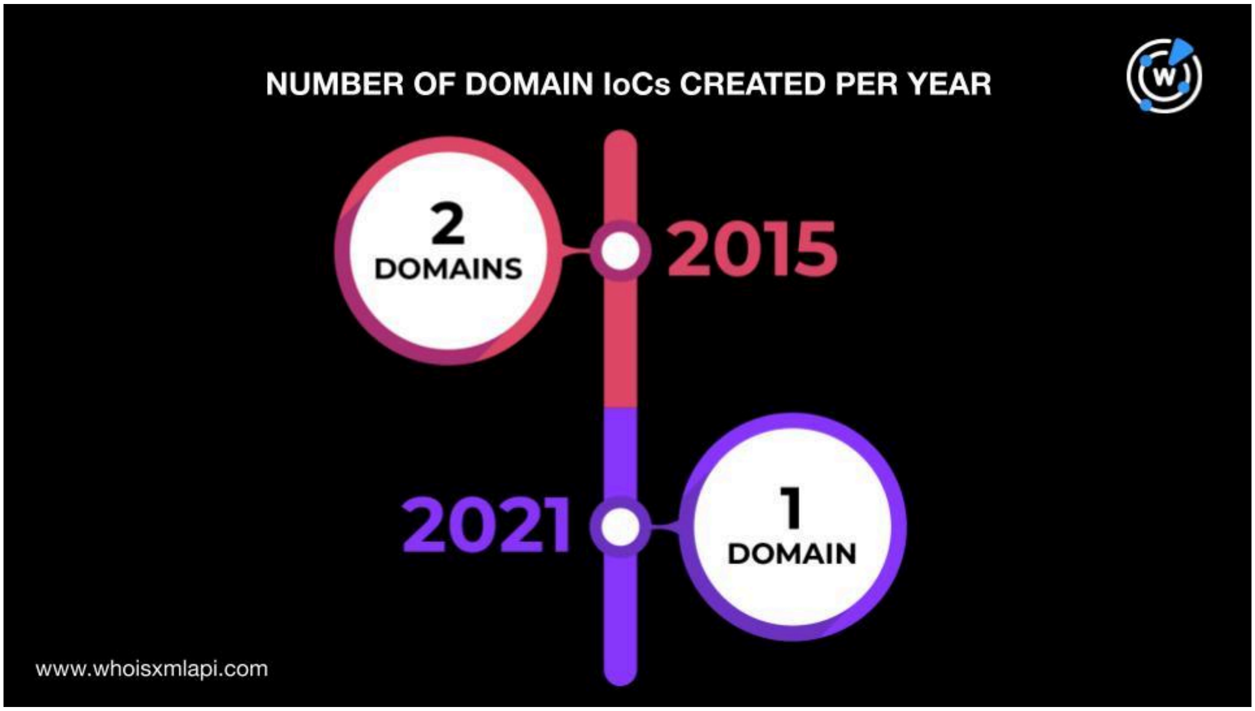
Samourai Wallet IoC Facts

We began our analysis by subjecting the three domains identified as IoCs to a bulk WHOIS lookup, which revealed that:

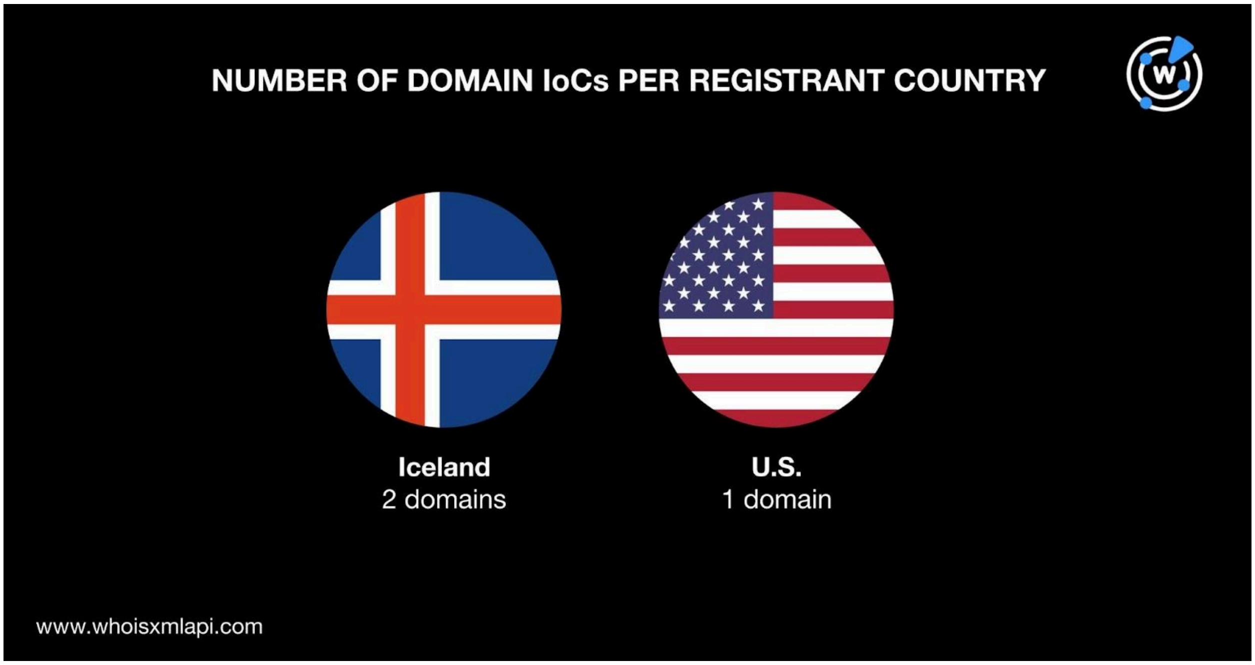
- They were split between two registrars. Namecheap, Inc. administered two domain IoCs while Gandi SAS handled one.



- The threat actors seem to prefer using old domains, created at the time the services were first offered, that is 2015. Two domain IoCs were created in 2015 while one was created in 2021.



- The domain IoCs were registered in two countries. Two were registered in Iceland and one in the U.S.



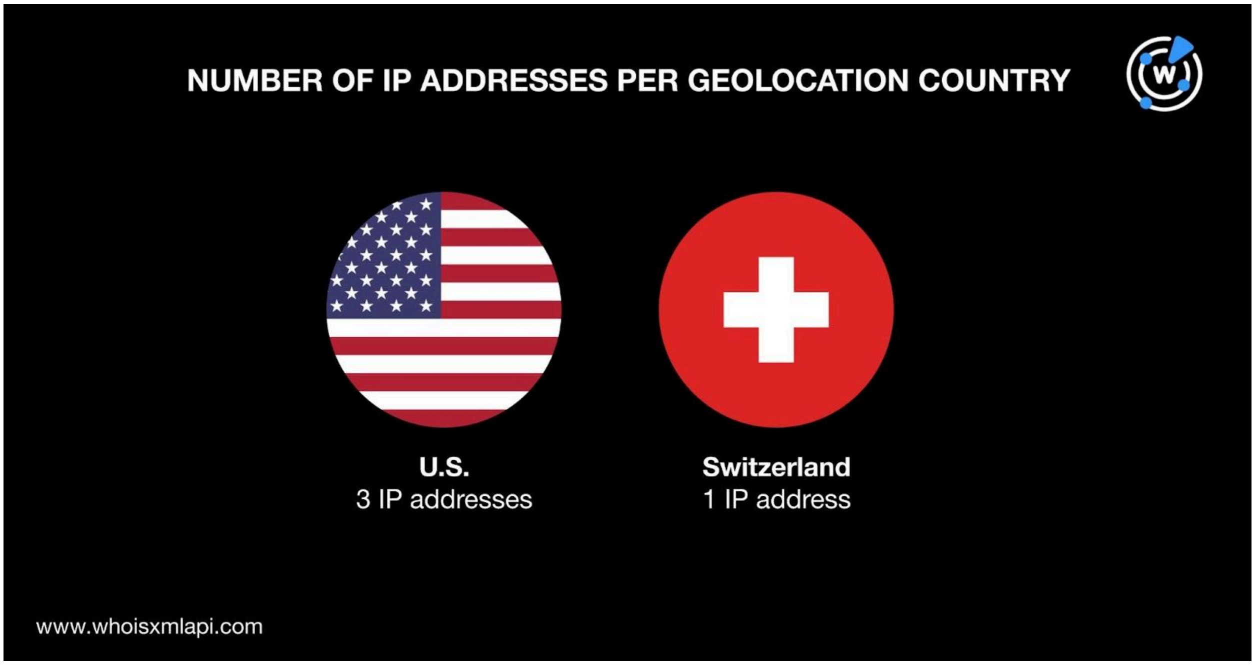
On to the Hunt for Connected Artifacts

We began our search for artifacts potentially connected to Samourai Wallet by conducting WHOIS History API queries for the three domains tagged as IoCs. That led to the discovery of three email addresses after duplicates were filtered out. None of them, however, were public email addresses, thus ending our search for email-connected domains.

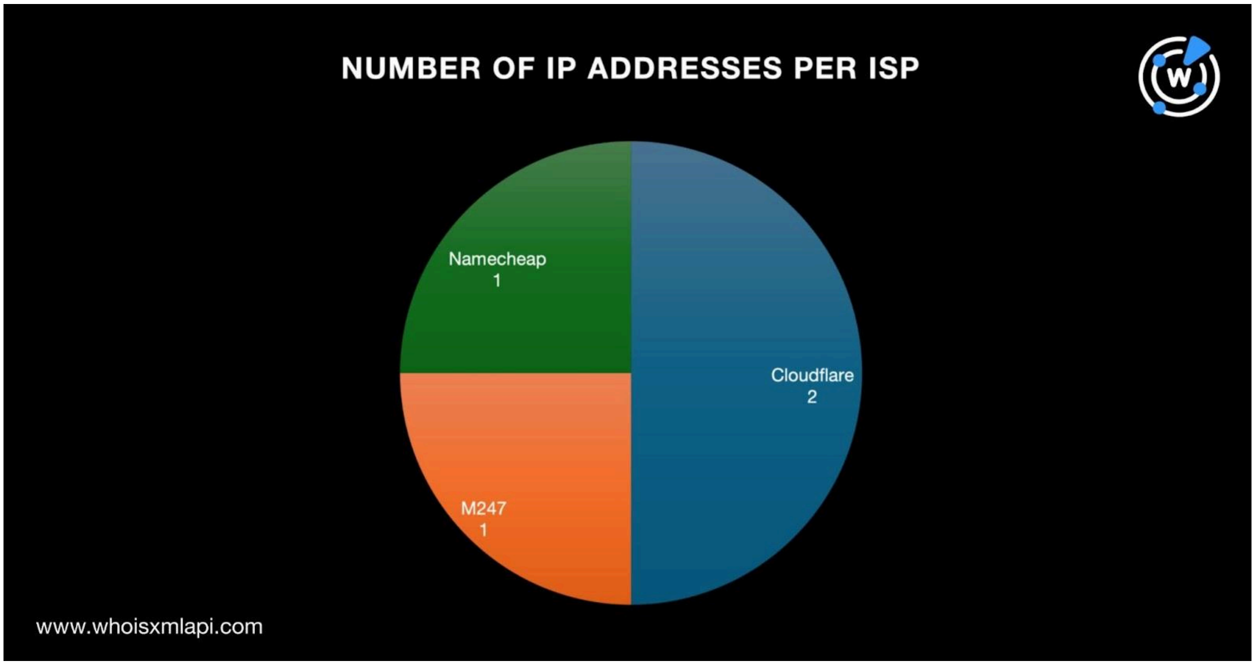
Next, we subjected the three domains identified as IoCs to DNS lookups, which enabled us to uncover four unique IP address resolutions. Threat intelligence lookups for the IP addresses showed that three—104[.]21[.]68[.]107, 162[.]255[.]119[.]8, and 172[.]67[.]194[.]72—were associated with various threats. The IP address 104[.]21[.]68[.]107, for instance, was linked to phishing and generic threats.

We then sought to uncover more information about the four IP addresses via a bulk IP geolocation lookup and found that:

- Three of the IP addresses are geolocated in the U.S. while the last one originated from Switzerland.


NUMBER OF IP ADDRESSES PER GEOLOCATION COUNTRY

- Cloudflare was the top ISP, accounting for two IP addresses. One IP address each, meanwhile, was administered by M247 and Namecheap.


NUMBER OF IP ADDRESSES PER ISP

Next, we queried the four IP addresses on Reverse IP Lookup and discovered that one of them—37[.]143[.]131[.]158—could be dedicated. It hosted two IP-connected domains, namely, samourai[.]email and samourai[.]is, after duplicates and the IoCs were removed. It is also interesting to note that they both had the text string **samourai**.

WHOIS lookups for the two IP-connected domains also revealed that:

- One of the IP-connected domains—samourai[.]email—shared the registrar Gandi SAS.
- Samourai[.]email and samourai[.]is shared the domain IoCs' creation years—2015 and 2021—as well.
- Interestingly, the current WHOIS record of the IP-connected domain samourai[.]is showed "Samourai LLC" as its registrant organization.

To ensure due diligence, we scoured the DNS for domains that started with the same text strings as the domains tagged as IoCs, namely:

- **samourai.**
- **samouraiwallet.**

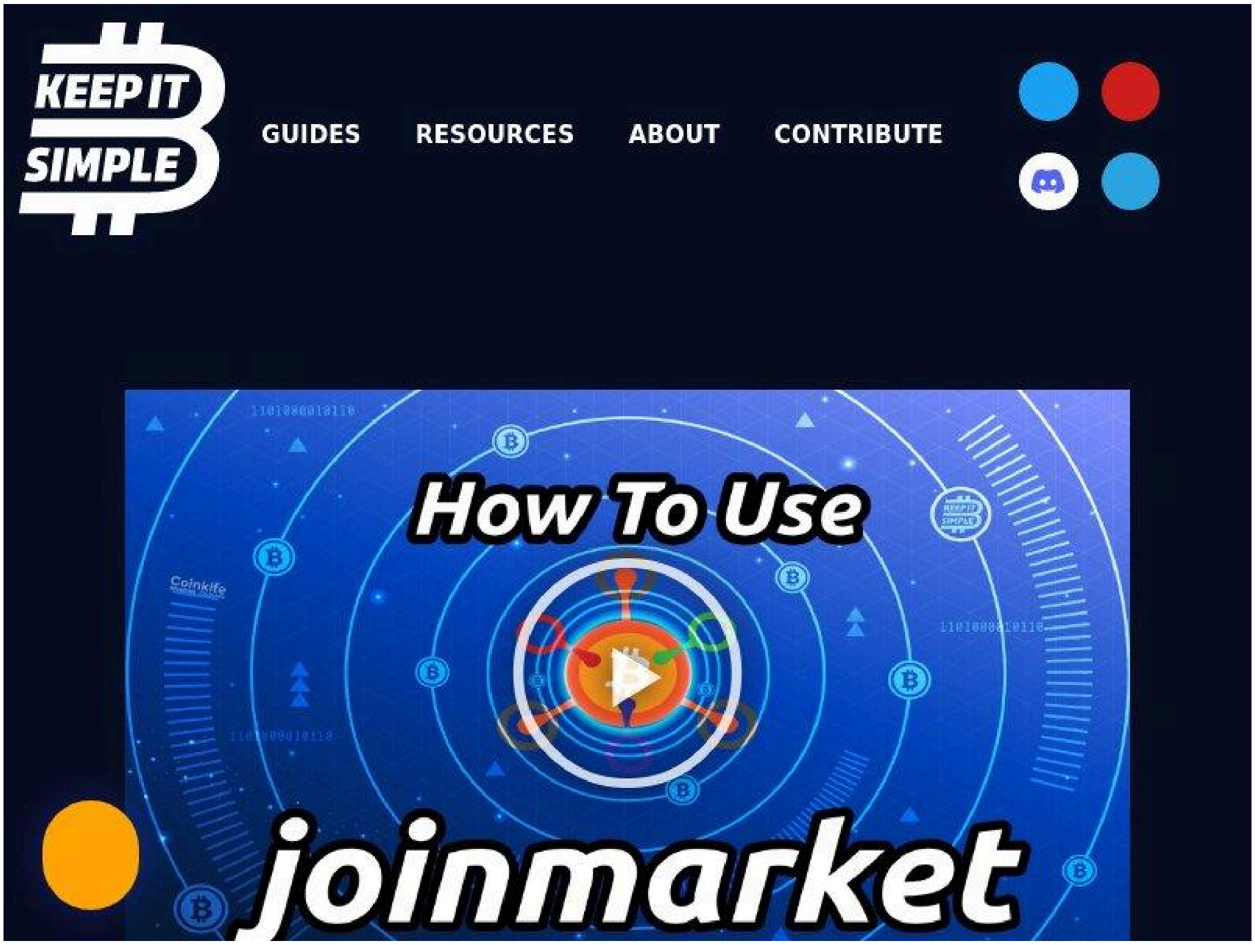
Our Domains & Subdomains Discovery searches led to the discovery of 66 string-connected domains after duplicates, the IoCs, and the IP-connected domains were filtered out.

A bulk WHOIS lookup for the 66 string-connected domains revealed similarities with the three domains identified as IoCs, such as:

- Five string-connected domains, namely, samourai[.]coop, samourai[.]store, samourai[.]tv, samourai[.]world, and samouraiwallet[.]fail, shared the domains IoCs' registrars (i.e., Gandi SAS and Namecheap, Inc.).
- Eight string-connected domains, namely, samourai[.]jp, samourai[.]info, samourai[.]co, samourai[.]ru, samourai[.]work, samourai[.]world, samouraiwallet[.]co, and samouraiwallet[.]org, shared the domain IoCs' creation years (i.e., 2015 and 2021).
- Fifteen string-connected domains, namely, samourai[.]club, samourai[.]com, samourai[.]live, samourai[.]finance, samourai[.]org, samourai[.]store, samourai[.]shop, samourai[.]us, samourai[.]xyz, samouraiwallet[.]ai, samouraiwallet[.]app, samouraiwallet[.]fail, samouraiwallet[.]net, samouraiwallet[.]sh, and samouraiwallet[.]org, shared the domain IoCs' registrant countries.
- It is also interesting to note that three string-connected domains, namely, samourai[.]coop, samourai[.]tv, and samourai[.]world, had something called "Cooperative Samourai," which is spelled very close to "samourai" in "Samourai Wallet," in the registrant organization field of their current WHOIS records.

While these findings do not necessarily point to direct connections with Samourai Wallet, the appearance of the text strings **samourai.** and **samouraiwallet.** in them and the similarities above seem suspect.

Of the 68 connected artifacts (i.e., IP- and string-connected domains combined), 28 remain accessible to date based on the results of Screenshot API queries. Take a look at an example below.



Screenshot of the page hosted on samouraiwallet[.]org

Based on the screenshot above, which displays Bitcoin logos, the content of the string-connected domain samouraiwallet[.]org seems connected to cryptocurrency—Samourai Wallet's business.

—

Our deep dive into Samourai Wallet using exhaustive DNS intelligence led to the discovery of 72 potentially connected artifacts comprising four IP addresses, two IP-connected domains, and 66 string-connected domains. Three of these artifacts—all IP addresses—were associated with phishing and generic threats. Many of them also had commonalities with the IoCs.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample IP Addresses

- 104[.]21[.]68[.]107
- 162[.]255[.]119[.]8

Sample IP-Connected Domain

- samourai[.]email

Sample String-Connected Domains

- samourai[.]app
- samourai[.]art
- samourai[.]be
- samourai[.]biz
- samourai[.]ca
- samourai[.]cf
- samourai[.]ch
- samourai[.]cloud
- samourai[.]club
- samourai[.]cn
- samourai[.]co
- samourai[.]co[.]jp
- samourai[.]co[.]uk
- samourai[.]com
- samourai[.]com[.]tw
- samourai[.]coop
- samourai[.]de
- samourai[.]dev
- samourai[.]digital
- samourai[.]eu