WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Framing the AkiraBot Framework Under the DNS Lens

Table of Contents

Executive Report

SentinelLABS recently dug deep into AkiraBot, a framework made to spam website chats and contact forms to promote a low-quality search engine optimization (SEO) service. So far, the bot has targeted 400K+ websites and spammed 80K+ websites since September 2024. According to the report, it uses OpenAI to generate custom outreach messages matching the target sites' purpose. Compared with typical spamming tools, it employs multiple CAPTCHA bypass mechanisms and network detection evasion techniques.

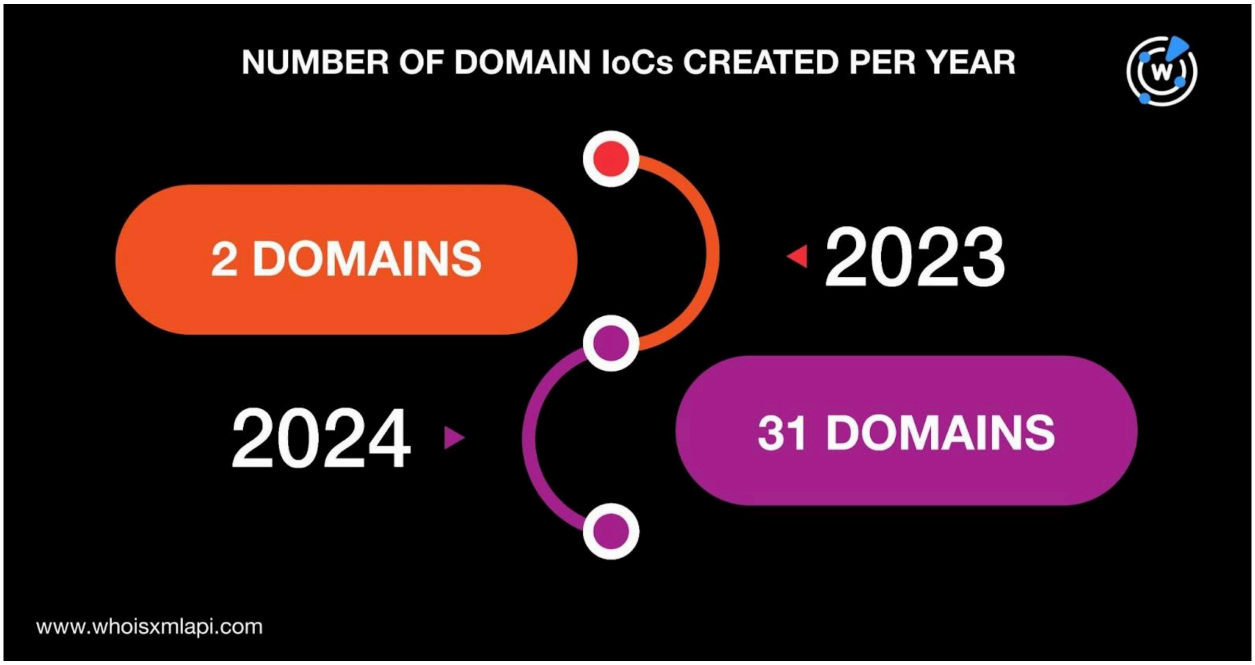
The researchers identified 34 domains as AkiraBot indicators of compromise (IoCs), which WhoisXML API expanded through a DNS deep dive that led to the discovery of:

- 16 email-connected domains
- 22 IP addresses, 10 of which turned out to be malicious
- 17 string-connected domains

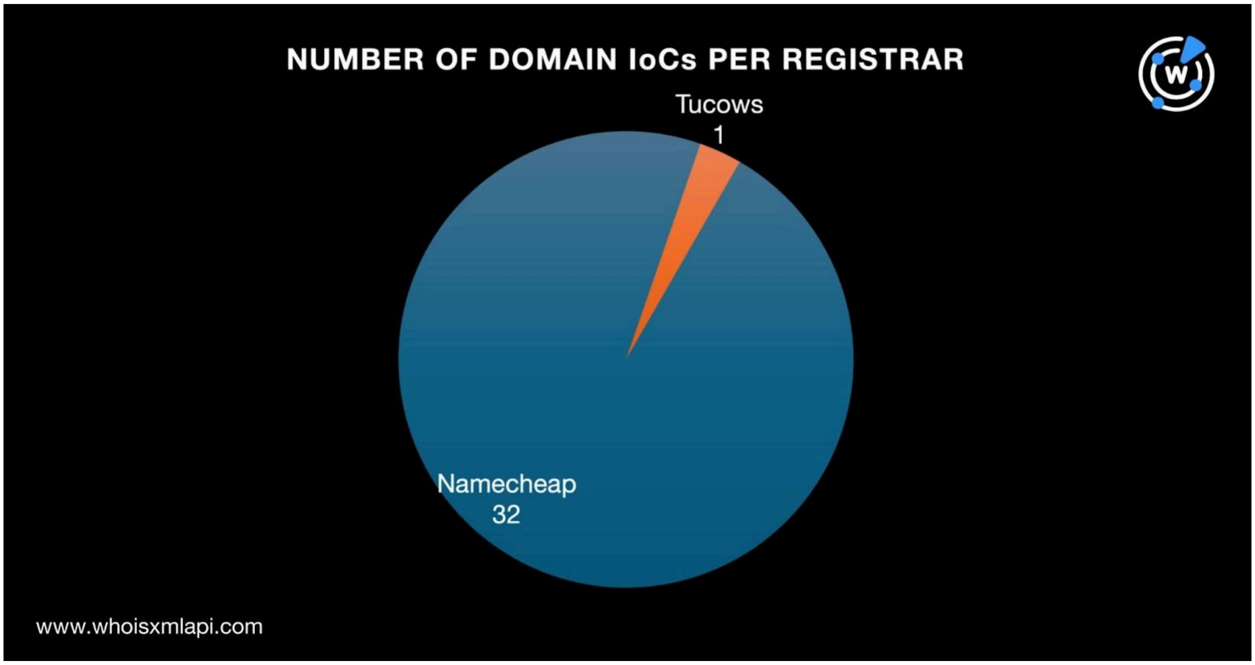
More on the AkiraBot IoCs

We began our information gathering by querying the 34 domains identified as IoCs on Bulk WHOIS API. We found that only 33 of the domains had current WHOIS records and:

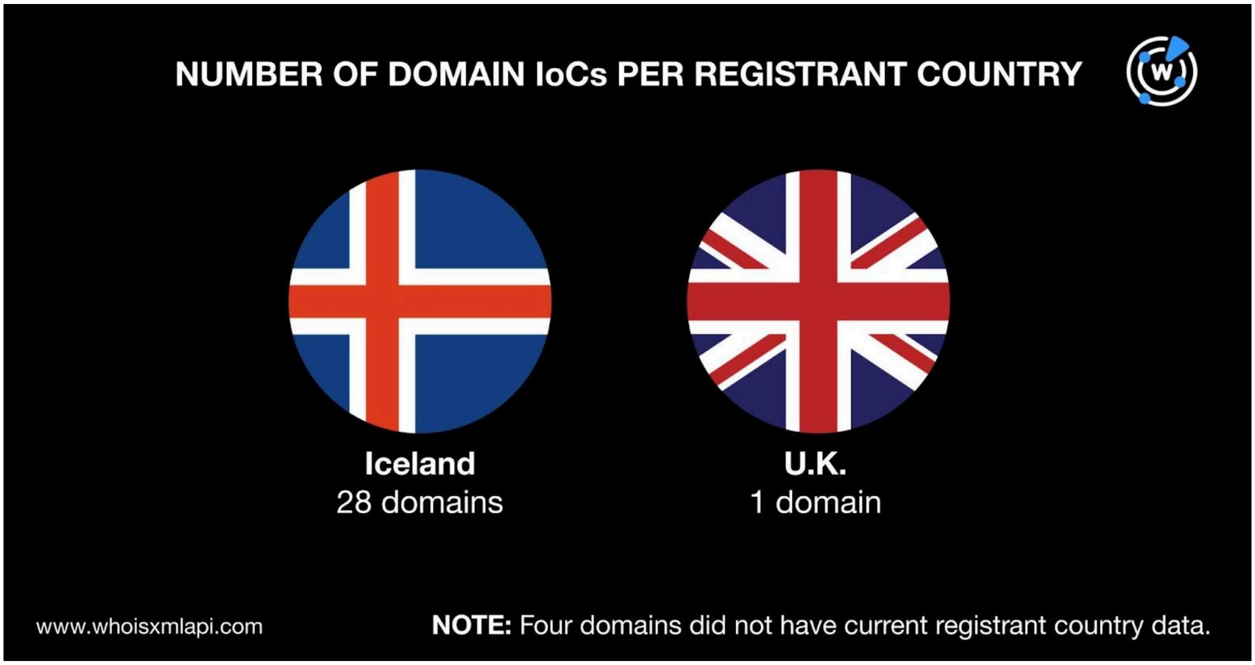
- They were created between 2023 and 2024 before they were weaponized for the September 2024 attacks.



- They were split between two registrars led by Namecheap, which accounted for 32 domains. Tucows administered one domain.



- Only 29 of the 33 domains with current WHOIS records had registrant countries. Specifically, 28 were registered in Iceland and one in the U.K.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

NOTE: Four domains did not have current registrant country data.

We also queried the 34 domains identified as IoCs on DNS Chronicle API and discovered that all of them had historical domain-to-IP resolutions. In fact, they recorded 359 resolutions over time. The domain letsgetcustomers[.]com posted the oldest resolution date, that is, to IP address 198[.]57[.]247[.]157 on 12 February 2017. Take a look at five other examples below.

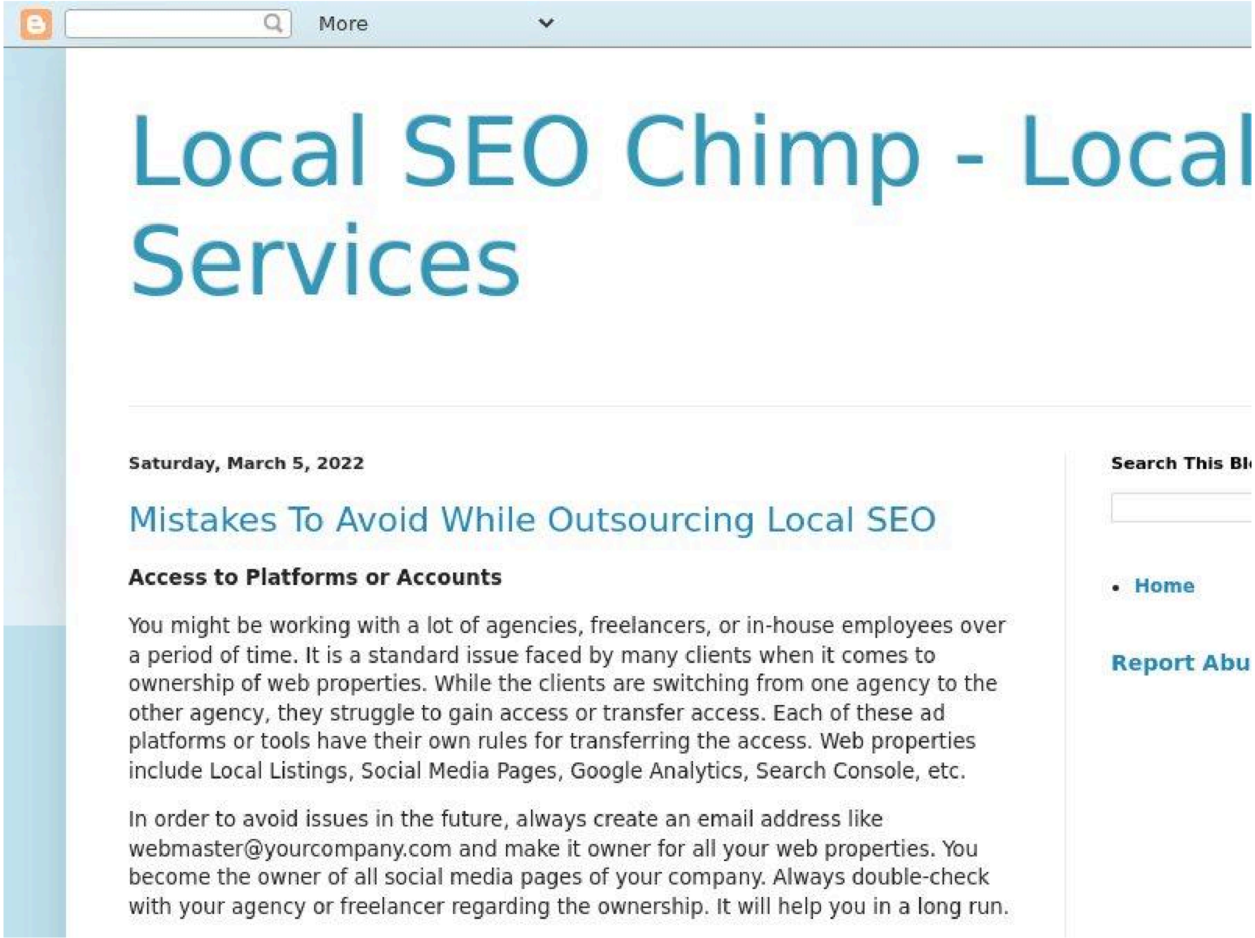
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
akirateam[.]com	19	6 June 2022
goservicewrap[.]com	30	4 April 2023
searchengineboosters[.]com	66	26 March 2023
servicewrap-go[.]com	17	12 September 2023
servicewrapgo[.]com	25	7 June 2023

Expanding the Current List of AkiraBot IoCs

To uncover artifacts possibly connected to the AkiraBot framework, we started by querying the 34 domains identified as IoCs on WHOIS History API. A total of 20 of the domains had 32 email addresses in their historical WHOIS records after duplicates were filtered out. Further scrutiny of the results unveiled three public email addresses.

We queried the three public email addresses on [Reverse WHOIS API]() afterward. While none of them appeared in the current WHOIS records of other domains, they were, however, present in the historical records of 16 email-connected domains after duplicates and those already identified as IoCs were filtered out.

A [Screenshot API]() query for the 16 email-connected domains showed that five continued to host live content. Possibly coincidentally, an example with the same theme as the IoCs—SEO services—is localseochimp[.]com.



Local SEO Chimp - Local Services

Saturday, March 5, 2022

Mistakes To Avoid While Outsourcing Local SEO

Access to Platforms or Accounts

You might be working with a lot of agencies, freelancers, or in-house employees over a period of time. It is a standard issue faced by many clients when it comes to ownership of web properties. While the clients are switching from one agency to the other agency, they struggle to gain access or transfer access. Each of these ad platforms or tools have their own rules for transferring the access. Web properties include Local Listings, Social Media Pages, Google Analytics, Search Console, etc.

In order to avoid issues in the future, always create an email address like webmaster@yourcompany.com and make it owner for all your web properties. You become the owner of all social media pages of your company. Always double-check with your agency or freelancer regarding the ownership. It will help you in a long run.

Screenshot of email-connected domain localseochimp[.]com

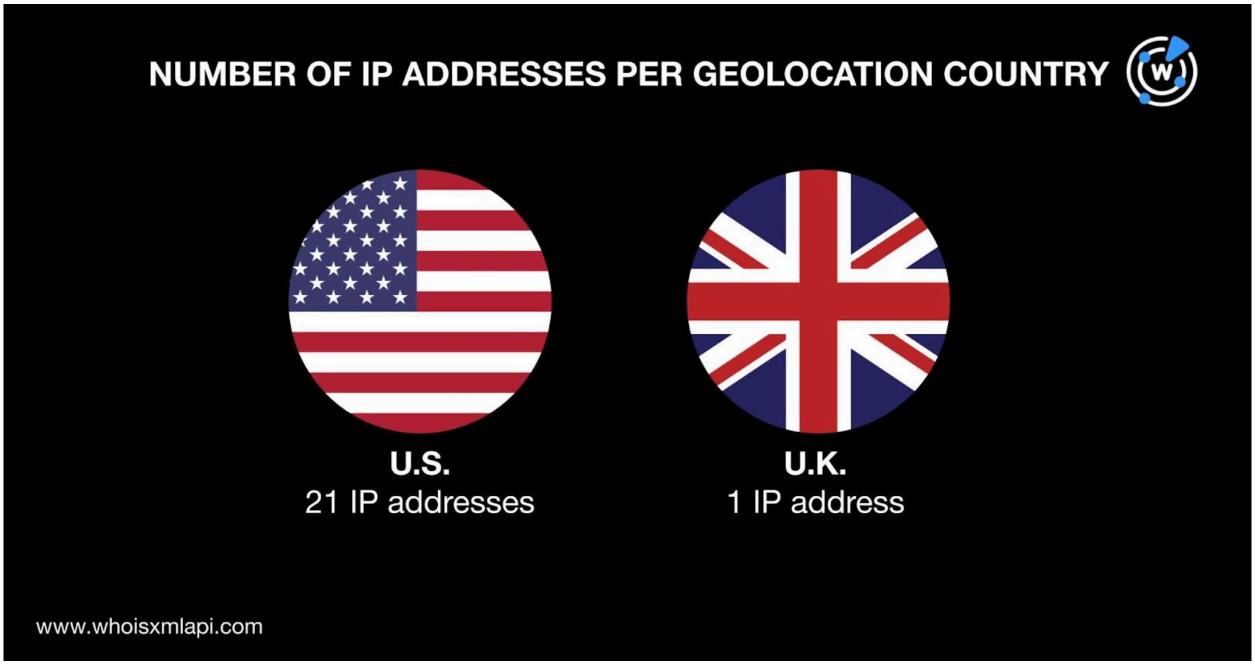
Next, we queried the 34 domains identified as IoCs on [DNS Lookup API]() and found that 33 of them actively resolved to IP addresses. In particular, the 33 domains resolved to 22 IP addresses after duplicates were filtered out.

A [Threat Intelligence API]() query for the 22 IP addresses revealed that 10 have already figured in various cyber attacks. Take a look at five examples below.

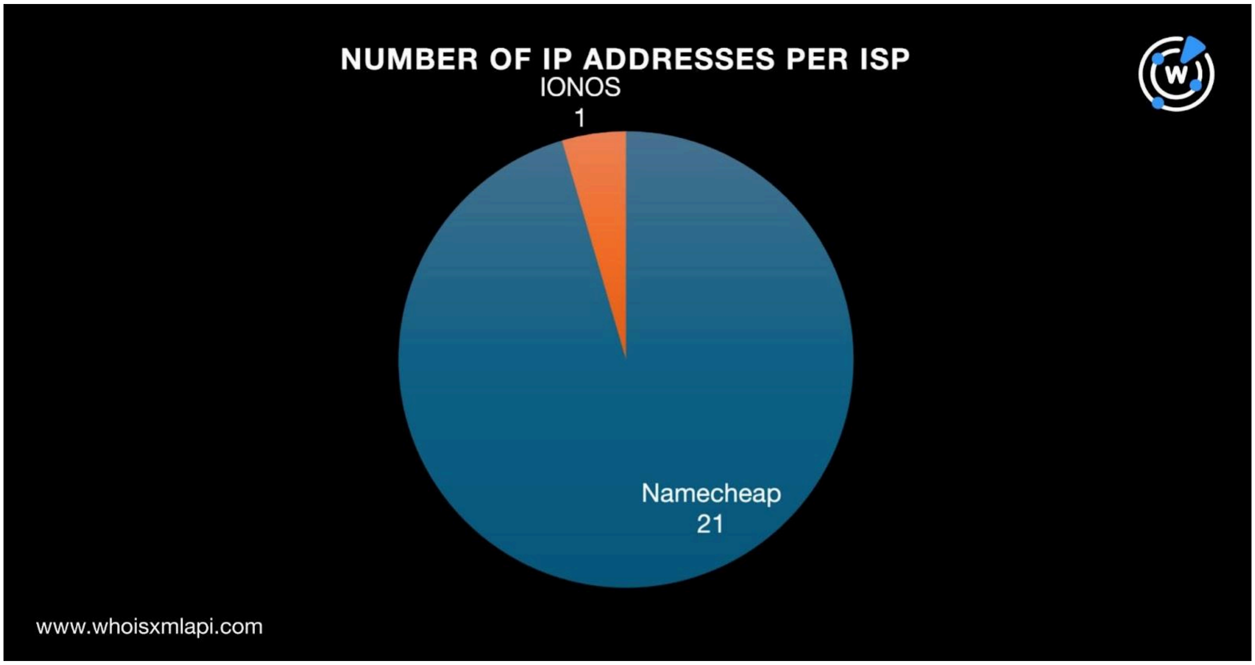
MALICIOUS IP ADDRESS	ASSOCIATED THREATS
162[.]213[.]251[.]17	Generic threat Malware distribution
198[.]187[.]31[.]121	Generic threat Malware distribution
198[.]187[.]31[.]163	Generic threat
198[.]54[.]114[.]248	Malware distribution
199[.]188[.]200[.]150	Attack Malware distribution Phishing

We also queried the 22 IP addresses on Bulk IP Geolocation Lookup and found that:

- They were geolocated in two countries led by the U.S., which accounted for 21 IP addresses. One IP address was geolocated in the U.K.



- They were split between two ISPs led by Namecheap, which accounted for 21 IP addresses. One IP address was administered by IONOS.

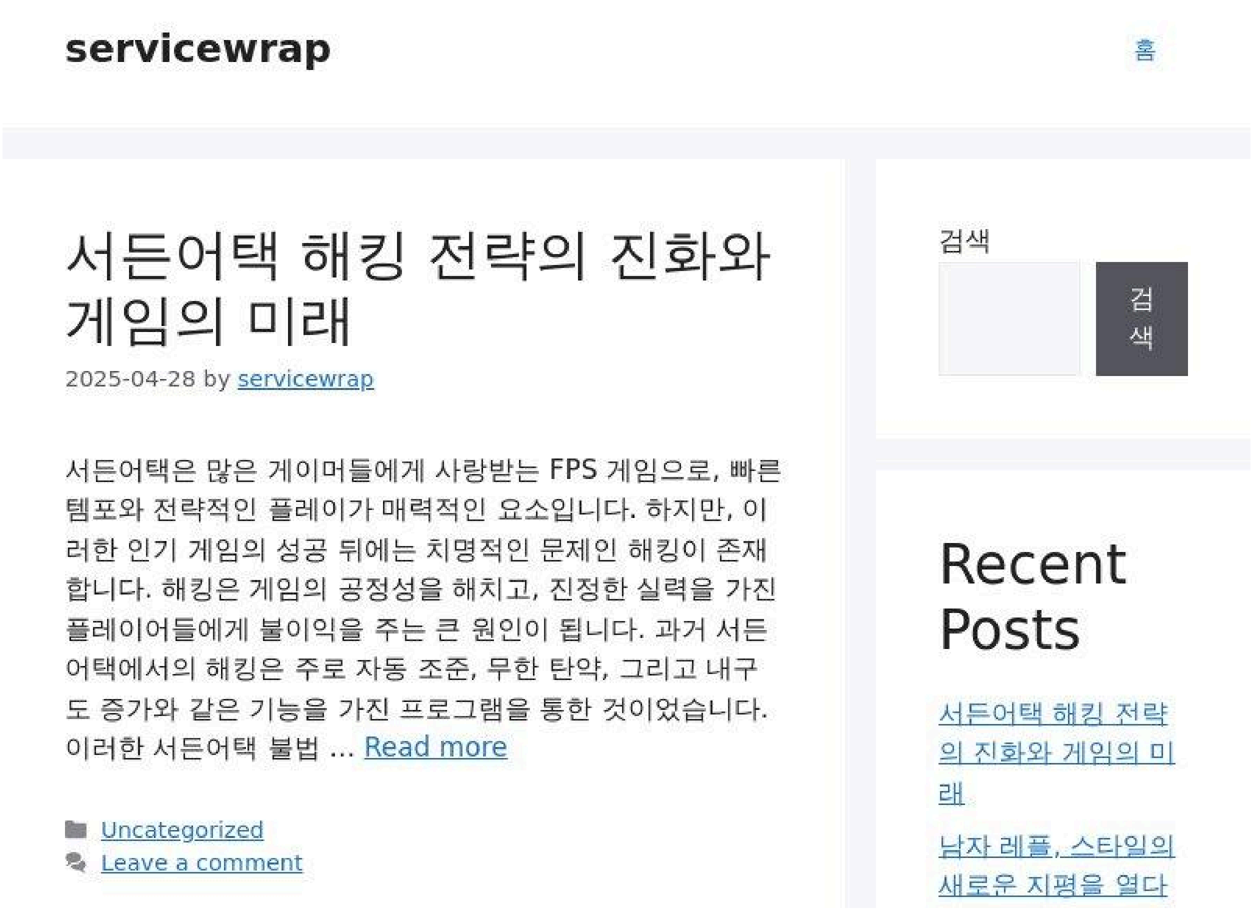


Next, a Reverse IP API query for the 22 IP addresses revealed that they hosted a total of 6,600 domains, translating to 300+ domains per IP. Unfortunately, none of the IP addresses were likely dedicated hosts, halting our search for IP-connected domains.

Our hunt for connected artifacts did not end there, though. We scoured the DNS for domains that contained the 34 text strings found among the domains identified as IoCs next. Our Domains & Subdomains Discovery searches using the **Starts with** parameter only showed results for these seven strings:

- akirateam.
- getkira.
- kiraone.
- onlyforyoursite.
- servicewrap.
- topservicewrap.
- usekiara.

Specifically, we uncovered 17 string-connected domains, only seven of which remained accessible to date according to the results of a Screenshot API query.



servicewrap

서든어택 해킹 전략의 진화와 게임의 미래

2025-04-28 by servicewrap

서든어택은 많은 게이머들에게 사랑받는 FPS 게임으로, 빠른 템포와 전략적인 플레이이가 매력적인 요소입니다. 하지만, 이러한 인기 게임의 성공 뒤에는 치명적인 문제인 해킹이 존재합니다. 해킹은 게임의 공정성을 해치고, 진정한 실력을 가진 플레이어들에게 불이익을 주는 큰 원인이 됩니다. 과거 서든어택에서의 해킹은 주로 자동 조준, 무한 탄약, 그리고 내구도 증가와 같은 기능을 가진 프로그램을 통한 것이었습니다. 이러한 서든어택 불법 … Read more

Recent Posts

- 서든어택 해킹 전략의 진화와 게임의 미래
- 남자 레플, 스타일의 새로운 지평을 열다

Screenshot of string-connected domain servicewrap[.]net

Other Possible Connections?

A closer look at the 34 domains identified as IoCs revealed similar text strings like **akira** and its possible variation **kira** as well as **servicewrap** and its variant **service-wrap**. Domains & Subdomains Discovery searches for the strings **akira** and **servicewrap** using the **Contains** parameter and limiting to domains created starting 1 September 2024 (when the campaign started) uncovered 2,016 domains.

While we could not determine if any of the 2,016 domains were owned by the same entities as the IoCs due to the former's record redaction, a closer look at their current WHOIS records showed that:

- 674 shared the domain IoCs' creation dates—between 2023 and 2024
- 243 shared the domain IoCs' registrars—Namecheap and Tucows
- 228 shared the domain IoCs' registrant countries—Iceland and the U.K.

—

Our in-depth DNS investigation into the AkiraBot framework led to the discovery of 55 potentially connected artifacts comprising 16 email-connected domains, 22 IP addresses, and 17 string-connected domains. In addition, 10 of the newly discovered artifacts have already been weaponized for various cyber attacks.

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 Email-Connected Domains

- babymusicaltoys[.]com
- homeshredded[.]com
- imgirlpower[.]com
- letsgetclients[.]com
- newbieanswers[.]com
- pineapplefitness[.]net
- revdigital[.]net
- shopetoy[.]com
- top10trustedreviews[.]com
- veteransjournal[.]org

Sample IP Addresses

- 162[.]0[.]215[.]192
- 162[.]0[.]215[.]5
- 162[.]213[.]251[.]17
- 66[.]29[.]141[.]223
- 67[.]223[.]118[.]103
- 67[.]223[.]118[.]105
- 77[.]68[.]64[.]40

Sample String-Connected Domains

- akirateam[.]net
- getkira[.]ai
- kiraone[.]com
- onlyforyoursite[.]ws
- servicewrap[.]cloud
- topservicewrap[.]services
- usekiara[.]com[.]br