DNS Investigation: Is xDedic Truly Done for After Its Takedown?

Table of Contents

Executive Report

Law enforcement agencies shut down xDedic, a cybercrime-as-a-service (CaaS) marketplace specifically providing web servers to cybercriminals, back in 2019. However, WhoisXML API threat researcher Dancho Danchev posits that parts of its backend infrastructure may remain traceable.

Our research team dove deep into the DNS in a bid to expand the list of 19 xDedic indicators of compromise (IoCs) Danchev provided, comprising three domains and 16 IP addresses, and determine if threat traces remained active. We uncovered:

- 15 email-connected domains, one of which turned out to be malicious
- 126 IP-connected domains, one of which turned out to be malicious
- Nine string-connected domains

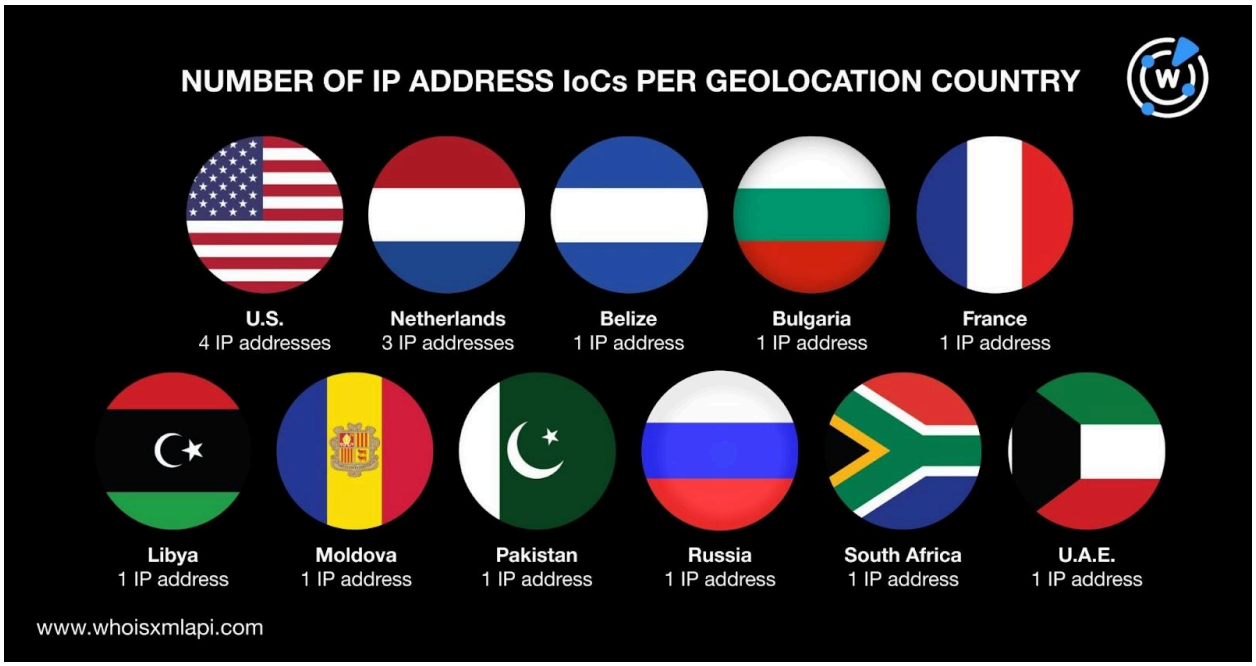
A Closer Look at the xDedic IoCs

As is our usual first step, we subjected the three domains identified as IoCs to a bulk WHOIS lookup that revealed that only one of the domain IoCs—xdedic[.]biz—had current WHOIS data, including:

- **Registrar:** PSI-USA, Inc.
- **Creation date:** 12 September 2014
- **Registrant country:** Canada

A bulk IP geolocation lookup, meanwhile, for the 16 IP addresses tagged as IoCs showed that:

- They were distributed among 11 geolocation countries led by the U.S., which accounted for four IP address IoCs. The Netherlands accounted for three IP address IoCs while one IP address each was geolocated in Belize, Bulgaria, France, Libya, Moldova, Pakistan, Russia, South Africa, and the U.A.E. The variety of IP address geographic locations could be due to the global nature of the threat.



- They were also spread across 13 ISPs led by Cloudflare, Inc., which accounted for four IP address IoCs. One IP address each was administered by 365 Online Technology Joint Stock Company, Alexhost SRL, Aljeel Aljadeed Technology, DIGIT1-IPOE, IQWeb FZ LLC, Liquid Telecommunications Operations Limited, Lirex.net, Multinet 125-101/24, OVH SAS, Pars Shabakeh Azarakhsh LLC, Serverius Holding B.V., and TOV Highload Systems.

Can xDedic Traces Still Be Found in the DNS?

Next, we sought to determine if xDedic traces remained even after the site had been shut down.

We began our IoC list expansion with WHOIS History API searches for the three domains classified as IoCs. They led to the discovery of five email addresses in the domain IoCs' historical WHOIS records. We used the only public email address to find email-connected domains.

Reverse WHOIS Search uncovered 15 domains with the email address in their historical WHOIS records. One email-connected domain—omerta[.]cc—according to Threat Intelligence API was associated with a malware attack.

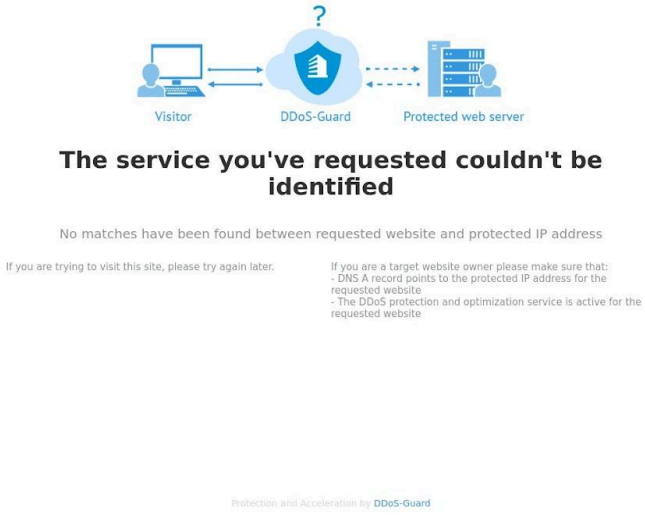
Three of the email-connected domains remained accessible to date based on screenshot lookup results. While one led to an error page, another was parked and the last led to a page with live content. The malicious email-connected domain omerta[.]cc was unreachable as of this writing.

Next, we performed DNS lookups for the three domain IoCs, which did not turn up IP addresses. But we could still look for IP-connected domains limited to the 16 IP address IoCs.

Reverse IP lookups for the 16 IP addresses named as IoCs showed that three of them—186[.]2[.]163[.]126, 87[.]236[.]215[.]18, and 91[.]220[.]101[.]43—could be dedicated. Altogether, they hosted 126 IP-connected domains after duplicates were filtered out.

Threat Intelligence API revealed that one IP-connected domain—vsoloviev[.]ru—was associated with generic threats.

According to Screenshot Lookup, the malicious IP-connected domain remained accessible despite leading to an error page as of this writing.



Screenshot of the page hosted on the malicious IP-connected domain vsoloviev[.]ru

Screenshot API queries for the 126 IP-connected domains also revealed that 117 remained accessible to date.

To round out our investigation, we also used Domains & Subdomains Discovery to look for other domains starting with the text string **xdedic.** We found nine string-connected domains.

A bulk WHOIS lookup for the **xdedic.**-containing domains revealed that:

- Five were administered by distinct registrars—ACTIVE-RU; Dynadot, Inc.; Eranet International Limited; GoDaddy.com LLC; and TurnCommerce, Inc. Four did not have current registrar data.
- A majority of them were created after the cybercriminal marketplace's takedown. Two domains were created in 2022 and one each in 2021 and 2023. Only one was created before 2019—xdedic[.]io—on 16 June 2016. Four did not have creation dates in their current WHOIS records.
- Three domains were registered in the U.S. and one in Saint Kitts and Nevis. Five did not have registrant countries in their current WHOIS records.

While none of the string-connected domains shared any similarity with the domain IoCs, one of them, xdedic[.]io, could be part of the underground marketplace's infrastructure or created for the operators' use given its creation date, which coincided with the site's heyday. Also, a Wayback Machine archived screenshot for xdedic[.]io showed that like the three domains identified as IoCs, it has been taken down by the authorities.

Screenshot of the page hosted on the IoCs xdedic[.]ac, xdedic[.]biz, and xdedic[.]tk as of 28 January 2019

Screenshot of the page hosted on the string-connected domain xdedic[.]io as of 1 February 2019

—

Our xDedic IoC list expansion led to the discovery of 150 potentially connected artifacts comprising 15 email-, 126 IP- and nine string-connected domains. One email- (i.e., omerta[.]cc) and one IP-connected domain (i.e., vsoloviev[.]ru) turned out to be malicious. In addition, the string-connected domain xdedic[.]io that remains in the DNS to date could potentially be part of the CaaS marketplace's infrastructure.

If you wish to perform a similar investigation or 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

- amtrustpills[.]com
- buycytotecnow[.]com
- buyingamoxicillin[.]com
- buyingclomid[.]com
- ed-generics-online[.]com
- goodfinance-blog[.]com
- gossipgel[.]com
- hotnpapers[.]com

Sample IP-Connected Domains

- abargrit[.]com
- ablb[.]ir
- ablbaspar[.]ir
- absanatco[.]com
- absanattehran[.]com
- alirantrading[.]net
- amnafza-co[.]ir
- apadanaart[.]com
- atbinfam[.]com
- atlasfilm[.]net
- atousaco[.]com
- balansanat[.]com
- bently[.]co
- betawin[.]ir
- binaloodpaint[.]com
- binaloodpaint[.]ir
- boghratlab[.]com
- cafechimney[.]ir
- candonama[.]com
- cheftco[.]com
- dkc-uae[.]com
- drkahnamuee[.]com
- drkahnamuee[.]ir
- ecoffice[.]co
- ecoffice[.]ir
- ecoffice[.]org

- elmisaz-autopart[.]com
- englandtour[.]ir
- fixopen[.]com
- goalelectric[.]co
- goalelectric[.]ir
- goalelectric[.]net
- gritpash[.]com
- haniantenna[.]com
- hseoic[.]com
- innopraktika[.]ru
- iran-oilshow[.]ir
- iran-watex[.]com
- iranaac[.]ir
- iranianhairclinic[.]com
- iriclub[.]com
- isfahan-elecomp[.]com
- kdd-group[.]com
- keshtsanatj[.]com
- kimia-pharma[.]co
- kish-tours[.]com
- kmcco[.]ir
- mandtgroup[.]co
- mashhademoghadas[.]com
- mashhademoghadas[.]ir

Sample String-Connected Domains

- xdedic[.]cc
- xdedic[.]club
- xdedic[.]com
- xdedic[.]in
- xdedic[.]io