WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A Peek at the V3B Phishing Kit Attack via the DNS Lens

Table of Contents

Executive Report

Phishing is and remains a top threat. Google alone blocks around 100 million phishing emails daily, and it doesn't help that phishers get extra help from phishing kits—ready-made cybercrime tools that allow even cybercriminal newbies to launch attacks following a few simple steps.

Resecurity recently uncovered a phishing campaign targeting the customers of several European banks aided by the V3B Phishing Kit. The company's research on the threat identified 28 domains as indicators of compromise (IoCs).

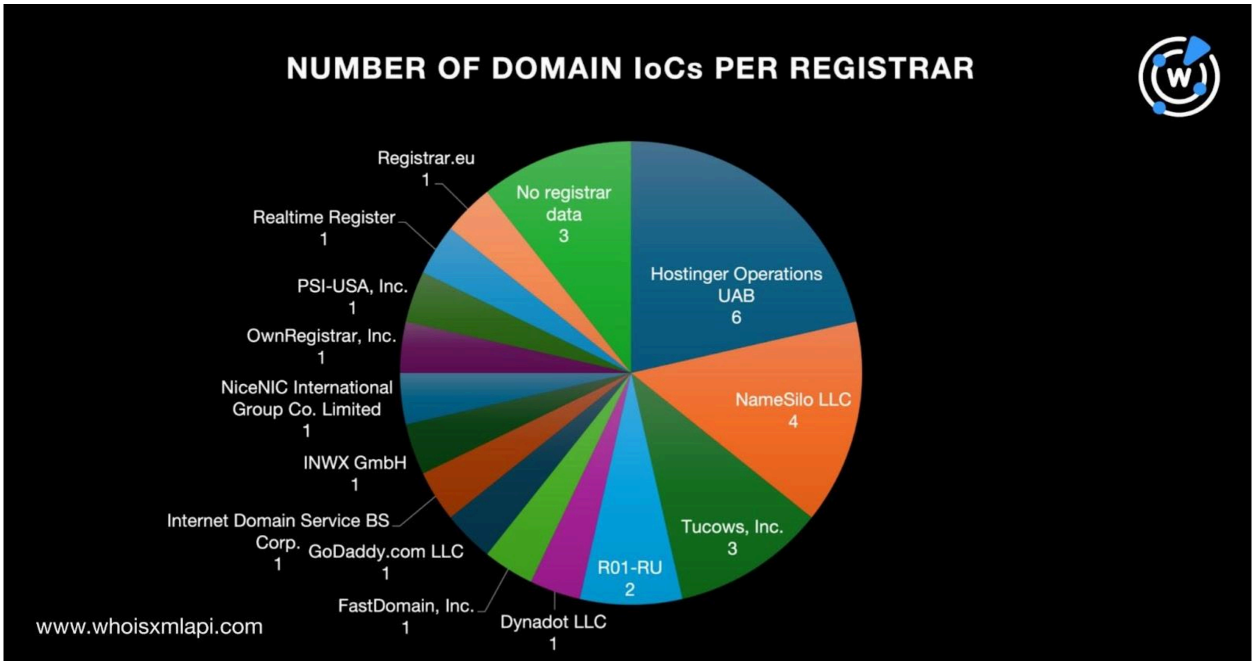
The WhoisXML API research team expanded the current list of IoCs in a bid to identify other potentially connected artifacts and found:

- 177 email-connected domains
- Nine IP addresses, eight of which turned out to be malicious
- 43 IP-connected domains
- 10 string-connected domains
- 32 brand-containing domains
- 4,537 registrant-connected domains, 490 of which were associated with various threats

IoC Facts

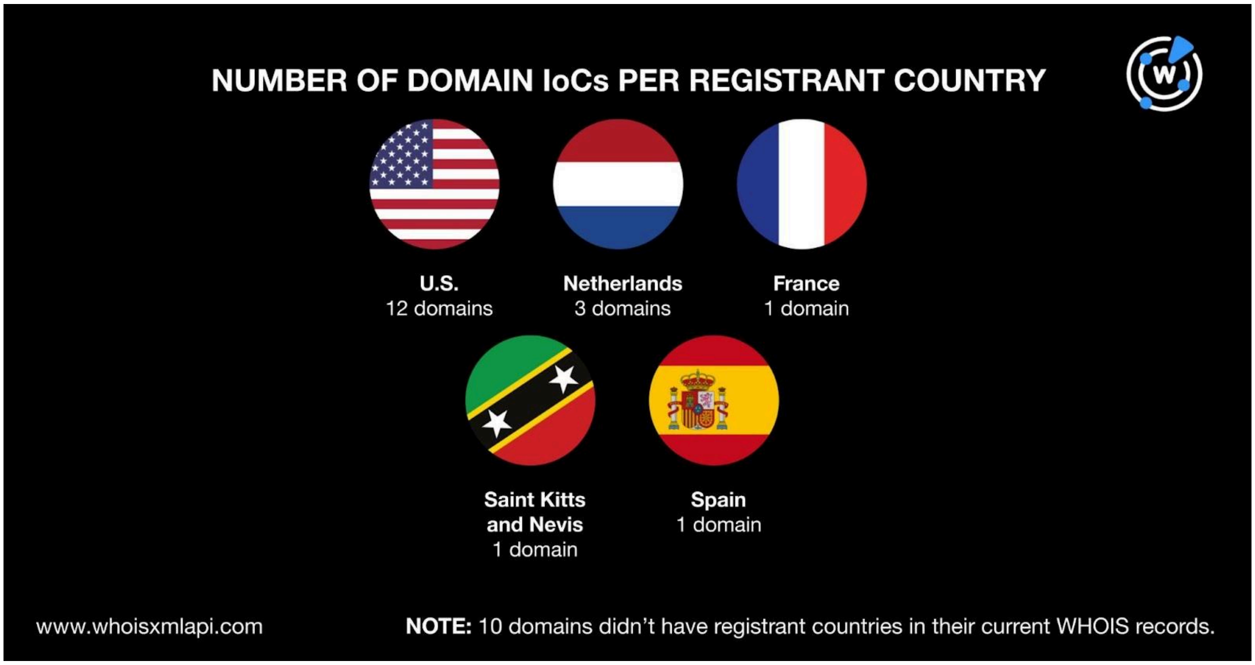
To find out more about the threat, we began by looking into the WHOIS records of the 28 domains tagged as IoCs via a bulk WHOIS lookup. Our query gave the following results:

- The domain IoCs were distributed among 14 registrars led by Hostinger Operations UAB, which accounted for six domains. NameSilo LLC administered four domain IoCs; Tucows, Inc. handled three; and R01-RU managed two. One domain each was administered by Dynadot LLC; FastDomain, Inc.; GoDaddy.com LLC; Internet Domain Service BS Corp.; INWX GmbH; NiceNIC International Group Co. Limited; OwnRegistrar, Inc.; PSI-USA, Inc.; Realtime Register; and Registrar.eu. Finally, three domain IoCs didn't have registrars in their current WHOIS records.



- The threat actors seemingly preferred to use newly registered domains (NRDs) given that 25 of the domain IoCs were created in 2024. Three of the domains didn't have creation dates in their current WHOIS records.

- The domain IoCs were registered in five countries led by the U.S., which accounted for 12 domains. The Netherlands took the second spot with three domain IoCs. France, Saint Kitts and Nevis, and Spain accounted for one domain each. Finally, 10 domain IoCs didn't have registrant countries in their current WHOIS records.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

NOTE: 10 domains didn't have registrant countries in their current WHOIS records.

- One domain IoC—bunq-app-nl[.]net—had public registrant name and organization data in its current WHOIS record.

IoC List Expansion Findings

We began our search for connected threat artifacts by querying the 28 domains tagged as IoCs on WHOIS History API. The query led to the discovery of 15 email addresses in their historical WHOIS records after duplicates were filtered out. Eight of the email addresses were public.

Reverse WHOIS API queries for the eight public email addresses revealed that they were present in the current WHOIS records of 177 email-connected domains after duplicates and the IoCs were removed.

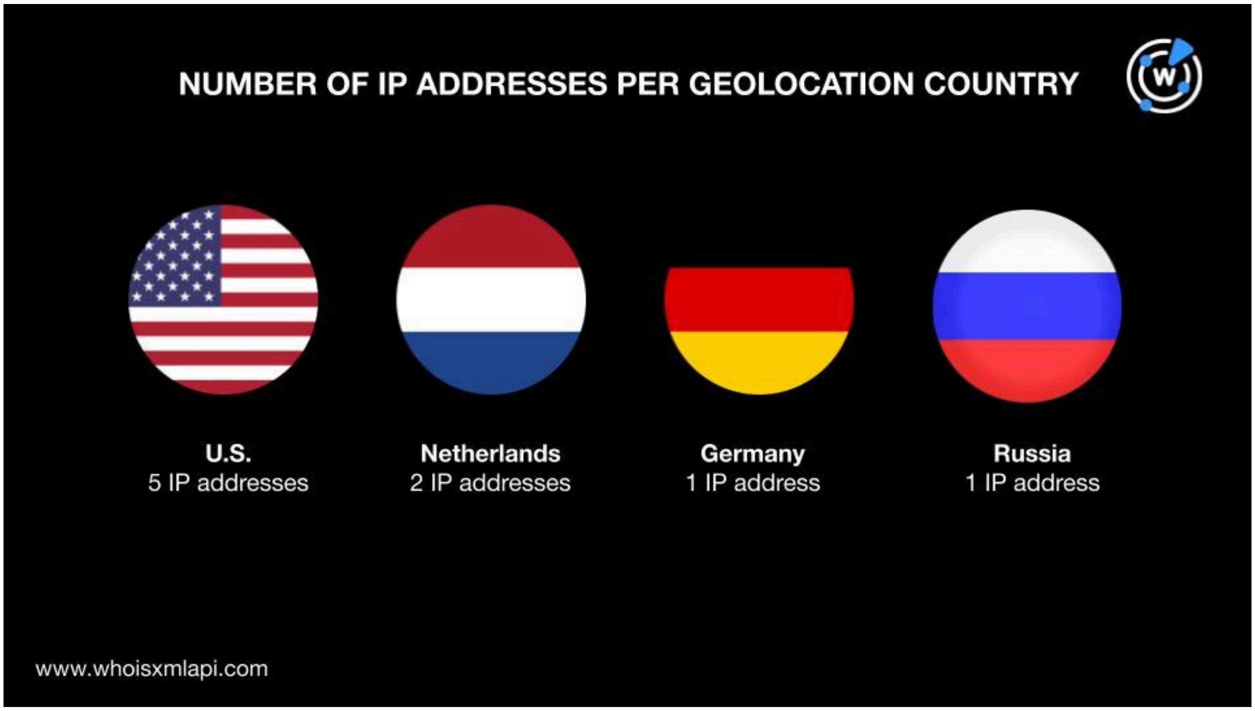
Next, we conducted DNS lookups for the 28 domains tagged as IoCs and found that they resolved to nine unique IP addresses, eight of which turned out to be associated with various threats according to Threat Intelligence Lookup. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]62[.]166	Command and control (C&C) Generic Malware Phishing

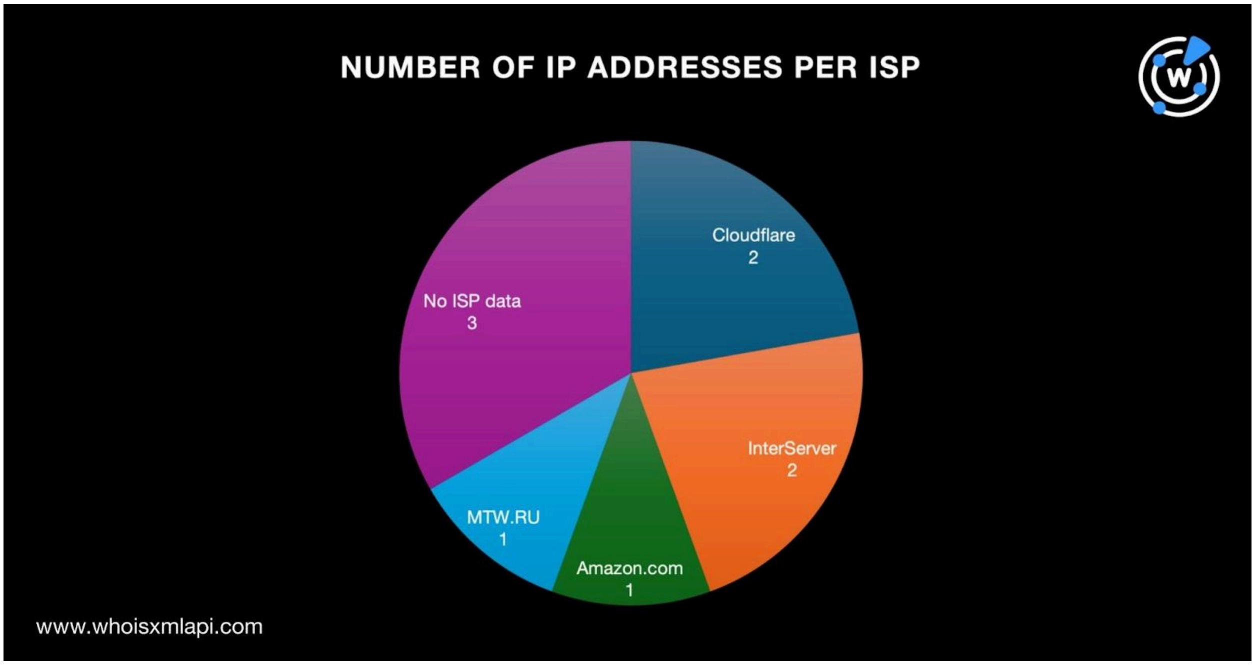
192[.]64[.]81[.]209	Attack Phishing Suspicious
45[.]141[.]101[.]36	Attack Malware
94[.]156[.]67[.]13	Attack Malware Spam
172[.]67[.]137[.]138	C&C Generic Malware Phishing

A bulk IP geolocation lookup for the nine public email addresses showed that:

- The U.S. was the top IP geolocation country, accounting for five IP addresses. The Netherlands took the second spot with two IP addresses. Finally, Germany and Russia accounted for one IP address each.



- The nine public IP addresses were distributed among four ISPs led by Cloudflare and InterServer, accounting for two IP addresses each. One IP address each was administered by Amazon.com and MTW.RU. Finally, three IP addresses didn't have ISP information in their A records.



Next, reverse IP lookups for the nine public IP addresses showed that four of them could be dedicated hosts. Altogether, they hosted 43 IP-connected domains after duplicates, the IoCs, and the email-connected domains were removed.

To find other possible connections, we used Domains & Subdomains Discovery to scour the DNS for domains that had the same text strings as the 28 domains tagged as IoCs. We found 10 string-connected domains that started with the five text strings below created on 1 January 2024 onward after duplicates, the IoCs, and the email- and IP-connected domains were filtered out:

- **black-loans7.**
- **icscards-nl.**
- **kontoaktualisierer-nl.**
- **kundenaktualisierungen.**
- **lcs-valideren**

Our closer look at the IoCs also revealed that the V3B Phishing Kit operators possibly set their sights on ABN AMRO Bank given the presence of the domain abn-amro-gobal[.]com in the IoC list. We looked for domains that started with the strings **abnamro** and **abn-amro** created in 2024. Our Domains & Subdomains Discovery queries provided 32 brand-containing domains—including abn-amro-1[.]top and abn-amro-coding[.]tech—after duplicates; the IoCs;

and the email-, IP-, and string-connected domains were removed. A bulk WHOIS lookup for the 32 brand-containing domains revealed that only one was owned by ABN AMRO Bank.

Earlier, we also mentioned that the domain IoC bunq-app-nl[.]net had public registrant name and organization data. We used those pieces of information to look for domains that had them in their current WHOIS records. We found 4,537 registrant-connected domains after duplicates; the IoCs; the email-, IP-, and string-connected domains; and the brand-containing domains were filtered out. Threat Intelligence API revealed that 490 registrant-connected domains were associated with various threats. Take a look at five examples below.

MALICIOUS REGISTRANT-CONNECTED DOMAIN	ASSOCIATED THREATS
0x0portal[.]com	Attack
aionitaruilib[.]xyz	Generic Phishing
airbnb-reservations22[.]com	Phishing
aruuliket[.]xyz	Phishing Generic
axs[.]claims	Attack

—

Our hunt for V3B Phishing Kit-connected web properties in the DNS allowed us to identify 4,808 threat artifacts. We also discovered that 89% of the IP addresses the domains tagged as IoCs resolved to were associated with various threats. In addition, 11% of the registrant-connected domains were malicious. Lastly, we found domains that phishers could potentially weaponize to target ABN AMRO Bank customers.

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

- aankoopverzekering[.]nl
- aanvraagbmwvisacard[.]nl
- aanvraageuroclixcard[.]nl
- aanvragencreditcard[.]nl
- accepteervisa[.]nl
- actualbeauty[.]nl
- aldipressmagezine[.]nl
- amsterdamaudio[.]nl
- apexboulders[.]nl
- asncreditcard[.]nl
- bdbracing[.]nl
- betaalgemak[.]nl
- betaalkaart[.]nl
- betaalmetapp[.]nl
- betaalmetvisa[.]nl
- bijenkorfcard[.]nl
- binnenstebuitencoaches[.]nl
- bmwvisacard[.]nl
- boulderhalenergiehaven[.]nl
- boulderhalkrachtstof[.]nl
- boulderhalkunstof[.]nl
- boulderhalkunststof[.]nl
- boulderhalroest[.]nl
- boulderhalzuidhaven[.]nl
- bouwstofbv[.]nl
- businesscard[.]nl
- businessgoldcard[.]nl
- businessmastercard[.]nl
- cardaanvragen[.]nl
- cashoncard[.]nl
- clixicon[.]com
- clixicon[.]nl
- corporatecard[.]nl
- corporatecreditcard[.]nl
- credit[.]nl
- creditcardonline[.]nl
- dagvandelosseverkoop[.]nl
- dbbusinesscard[.]nl
- dbbusinesscards[.]nl
- dbcorporate[.]nl
- dbcorporatecard[.]nl
- de-sitter[.]nl
- debijenkorfcard[.]nl
- dekookvogels[.]com
- dekookvogels[.]nl
- delicatess[.]nl
- denken-doen[.]nl
- derembrandtcode[.]nl
- devschuur[.]nl
- dockmasters[.]nl

Sample IP-Connected Domains

- 0wadbe[.]ru
- 30dfka3[.]ru
- 3824eee[.]ru
- 6qc2up[.]ru
- 705hgs[.]ru
- 8tzqeg[.]ru
- b3qymx[.]ru
- bitvavo-controleren[.]com
- bitvavo-verificatie[.]com
- bitvavoverificatie[.]com
- c300qa4[.]ru
- csk0t5[.]ru
- daredevildog[.]net
- dpaf23[.]ru
- dqou0e[.]ru
- emgt0y[.]ru

- fz2zot[.]ru
- lh0ihn[.]ru
- m20wld[.]ru
- nlbltvavo[.]com

Sample String-Connected Domains

- belastingdienst-schuld[.]ru
- belastingoverzicht[.]nl
- black-loans7[.]club
- black-loans7[.]life
- black-loans7[.]services

Sample Brand-Containing Domains

- abn-amro-1[.]top
- abn-amro-coding[.]tech
- abn-amro-online[.]top
- abn-amro[.]in
- abn-amro[.]link
- abnamro-invest[.]com
- abnamro[.]com[.]co
- abnamro[.]ml
- abnamro[.]pics
- abnamroapp[.]com
- abnamrobanking[.]com
- abnamroclearing[.]au
- abnamroi[.]nl
- abnamroline[.]cc
- abnamroline[.]com
- abnamroline[.]one

Sample Registrant-Connected Domains

- 0-spk[.]info
- 02-kundenportal[.]info
- 02-vertrag[.]info
- 04718459-coinbase[.]com
- 0p-asiakaspalvelu[.]com
- 0p-etusivu-fi[.]info
- 0p-fi[.]com
- 0x0portal[.]com
- 0x45375677x[.]sbs
- 1-everbridge[.]com
- 17937429-coinbase[.]com
- 17986429-coinbase[.]com
- 18047265-coinbase[.]com
- 1inch[.]claims
- 1inch[.]gifts
- 1inchs[.]network
- 1innch[.]digital
- 1stcoin[.]in
- 1yagodame[.]com
- 2023crafilings[.]site
- 2fa-connect[.]app
- 6271872[.]live
- 70346931-confirm[.]com
- 7498[.]info
- 79137431-coinbase[.]com
- 9138[.]info
- 9183[.]info
- 9594[.]info
- 9862334-confirm[.]com
- 986395-confirm[.]com
- 9865234-confirm[.]com
- 987134-confirm[.]com
- a-everbridge[.]com
- a1-mobile[.]app
- aave-survey[.]net
- aave-survey[.]org
- aave[.]gifts
- aaveform[.]com

- aavenetworks[.]com
- aaveportal[.]net
- abanca-acceso-empresas[.]com
- abanca-alertas[.]app
- abanca-empresas[.]co
- abanca-empresas[.]digital
- abanca-empresas[.]net
- abanca-es[.]digital
- abanca-seguridad-movil[.]digital
- abanca-seguridad[.]digital
- abn-authoriseren[.]com
- acc-fl[.]com
- acc-ld[.]com
- accedibnl[.]in
- acceso-login[.]sbs
- acceso-seguro[.]sbs
- acceso[.]mobi
- accesso-mediolanum[.]in
- account-support-coinbase[.]com
- actualizar[.]sbs
- added-inspect[.]com
- adesion-web-portale-it[.]xyz
- adesione-web-it[.]xyz
- adesione-web[.]com
- adidas-baseorg[.]com
- adidasbase[.]org
- admin-govdelivery[.]com
- administracion-gob-es[.]app
- adresseidentite[.]info
- aeithirclouds[.]xyz
- aerodrome-fi[.]net
- aethir-airdrop[.]com
- aethircioud[.]com
- aethirclouds[.]com
- aethirfi[.]com
- aethirfinance[.]com
- aethirlab[.]com
- aethirlabs[.]app
- aethirlabs[.]net
- aethrcloud[.]com
- aevvo[.]co
- ag-post[.]com
- agencia-tributaria[.]digital
- agoda-offer11279[.]com
- agoda-offer18239[.]com
- agos-ducato[.]com
- ai-trezor[.]io
- aiblivechat[.]com
- aieo[.]app
- aiiocate-biasti2[.]app
- aiiocate-biasti2[.]net
- aiiocate-biastl2[.]app
- aiiocate-biastl2[.]net
- aiiocate-blastl2[.]app
- aiiocate-blastl2[.]net
- aiiocate-debank[.]app
- aiiocate-debank[.]com
- aiiocate-debank[.]net
- aiiocate-debankfl[.]net
- aiiocate-dop[.]net
- aiiocate-layerzerolab[.]com
- aiiocate-milkywayzone[.]com