BlackCat Hacks Reddit Again, Take a Look at What the DNS Revealed

Table of Contents

Executive Report

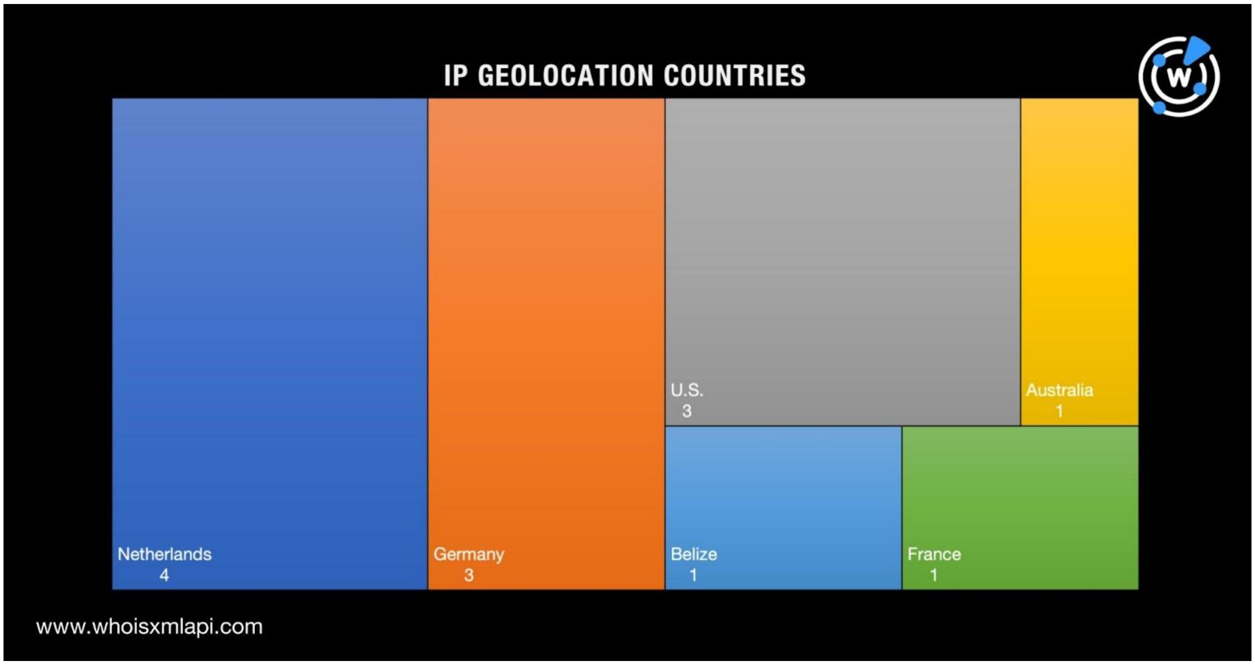
The first time the BlackCat ransomware gang breached Reddit's network last February, they phished an employee to hack into the target network. This time, according to a ReversingLabs detailed report, they successfully dropped BlackCat onto the company's systems and threatened to release its data if it fails to pay the ransom.

In WhoisXML API's bid to make the Internet more transparent and safer for all users, we expanded the list of indicators of compromise (IoCs) comprising 13 IP addresses published on 4 June 2023. Our comprehensive DNS searches for traces the threat group may have left behind uncovered:

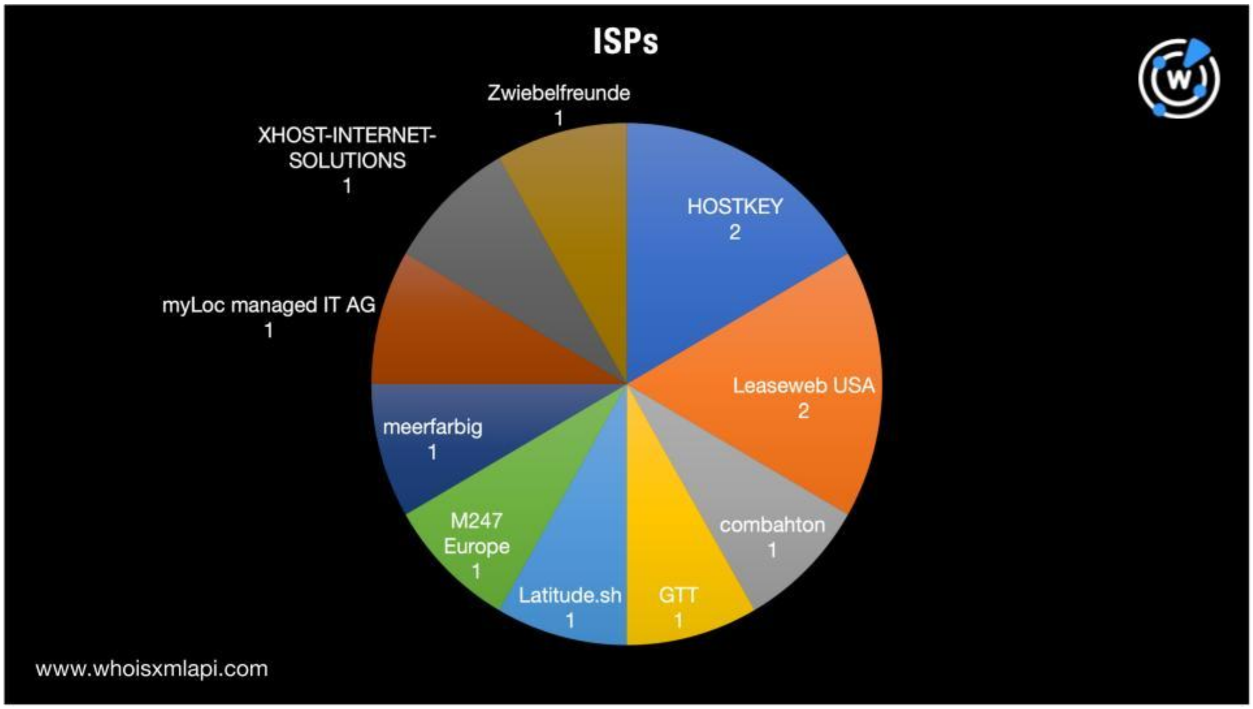
- Three domains hosted on two dedicated IP addresses identified as IoCs
- 437 domains containing the string **office365logs**, **off365**, or **office365** akin to the closely related IP-connected artifact off365logs[.]online, 53 of which have been classified as malicious based on a bulk malware check
- 20 domains containing the string **rbcbank** akin to the closely related IP-connected artifact secure-rbcbank[.]net, two of which have been categorized as malicious based on a bulk malware check

IoC-Related Findings

A bulk IP geolocation lookup for the IoCs revealed that they were geographically distributed across six countries led by the Netherlands, which accounted for four of the IP addresses. Germany and the U.S. tied in second place, accounting for three IP addresses each. Australia, Belize, and France completed the list, each accounting for one IP address.



Further scrutiny showed the IoCs were spread across 10 ISPs led by HOSTKEY, Leaseweb USA, and M247 Europe, which accounted for two IP addresses each. Combahton, GTT, Latitude.sh, Meerfarbig, myLoc managed IT AG, Xhost Internet Solutions, and Zwiebelfreunde rounded out the list, each accounting for one IP address.

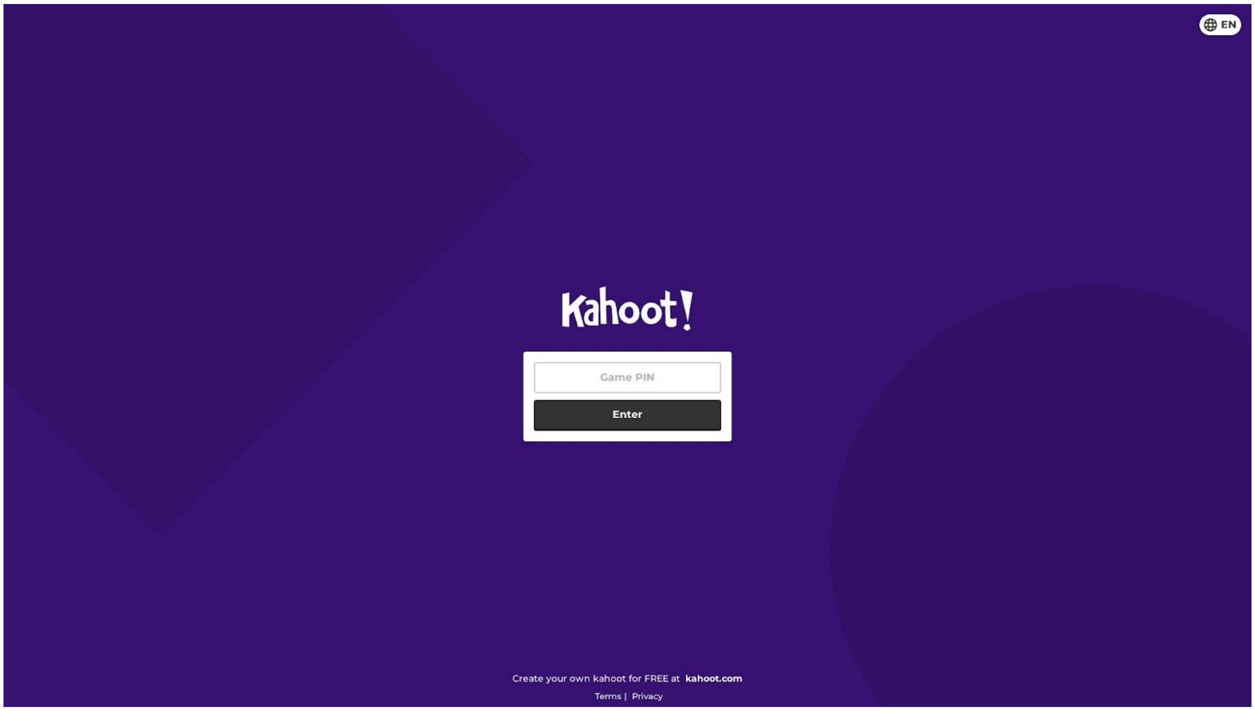


Pivoting Off the IoCs

We began our DNS deep dive with reverse IP lookups for the IoCs, which allowed us to determine that two of them were dedicated hosts. Together, 89[.]44[.]9[.]243 and 185[.]220[.]102[.]253 hosted three domains. While two out of three of the IP-connected domains continued to host live content, one turned out to be a Tor exit node. The other two appeared to be cybersquatting properties based on their domain names alone.

The first, off365logs[.]online, could be passing itself off as a Microsoft-owned Office 365 page though it's parked at present. Its WHOIS record, however, didn't bear any similarity to that of microsoft[.]com. In particular, it didn't share the legitimate domain's registrar and registrant email address.

The second, secure-rbcbank[.]net, could be pretending to belong to Canada-based RBC Bank. Like the first potential cybersquatter, it, too, didn't have the same WHOIS record details as rbcbank[.]com. Its screenshot also shows a Kahoot! login page.



Create your own kahoot for FREE at **kahoot.com**

Screenshot of secure-rbcbank[.]net

Both potentially cybersquatting sites aren't considered malicious to date but threat actors could easily weaponize them for attacks targeting Office 365 users and RBC Bank customers. It's also interesting to note that secure-rbcbank[.]net's current WHOIS record contained an unredacted registrant email address that may help security researchers and law enforcement agencies conduct more in-depth investigations.

To gather more artifacts, we looked for domains containing the names of the brands that could also belong to the threat actors behind BlackCat ransomware.

Our Domains & Subdomains Discovery searches for domains containing the string **office365logs**, **off365**, or **office365** created since 1 January 2023 that could be weaponized to target Office 365 users allowed us to uncover 437 such web properties. A bulk WHOIS lookup for the Office 365 string-connected domains revealed that only three of them could be publicly attributed to Microsoft based on their registrant email address. A bulk malware check, meanwhile, showed that 53 of them were tagged as malicious. Here are other interesting findings:

- While five of the string-connected domains had the same registrar as the legitimate Microsoft domains (uwu[.]ai, toolforge[.]org, office365[.]com[.]pr, azurestaticapps[.]net, and office365login[.]co[.]il), only three of them were confirmed to be Microsoft-owned (office365[.]com[.]pr, azurestaticapps[.]net, and office365login[.]co[.]il).
- 260 of the domains were created just this year.
- The U.S. was the top registrant country, accounting for 129 of the domains. Canada and China completed the top 3 registrant countries, accounting for 70 and 12 domains, respectively.

Next, we performed a similar search for domains containing the string **rbcbank** created in the same period and found 19 such web properties. Unlike some of the Office 365 string-connected domains, none of them could be publicly attributed to RBC Bank. Also, two of them have been tagged as malicious based on a bulk malware check. Here are other noteworthy findings:

- None of the RBC Bank string-connected domains had the same registrar as rbcbank[.]com.
- A majority of the domains, 18 to be exact, were created just this year.
- The U.S. was the top registrant country, accounting for nine of the domains. Canada accounted for three domains, the Netherlands and Seychelles accounted for two each, and Uzbekistan for one.

—

Further scrutiny of the latest BlackCat attack on Reddit led to the discovery of 460 yet-unpublished artifacts with close IP connections to and string similarities with the IoCs. A total of 55 of the newly found domains may have already figured in cyber attacks or phishing campaigns, given that they are currently being detected as malicious by a malware checker. A huge majority of the artifacts could also easily be weaponized for other attacks specifically targeting Office 365 users and RBC Bank customers.

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 and IoCs

IP Addresses Identified as IoCs

- 89[.]44[.]9[.]243
- 142[.]234[.]157[.]246
- 45[.]134[.]20[.]66
- 185[.]220[.]102[.]253
- 37[.]120[.]238[.]58
- 152[.]89[.]247[.]207
- 198[.]144[.]121[.]93
- 89[.]163[.]252[.]230
- 45[.]153[.]160[.]140
- 23[.]106[.]223[.]97
- 139[.]60[.]161[.]161
- 146[.]0[.]77[.]15
- 94[.]232[.]41[.]155

Sample Domains Hosted on the Dedicated IP Addresses Identified as IoCs

- off365logs[.]online
- secure-rbcbank[.]net

Sample Office 365 String-Connected Domains

- off365vn[.]com
- msoff365[.]online
- standoff365[.]com[.]de
- nodaysoff365[.]co[.]uk
- off365portl[.]online
- admnoff365teams[.]com
- off365app23duo2fa365online[.]com
- exch-mail-off365svr-mrosfs1t[.]com
- svr-365-01server-off365svr-mrosfs1t[.]com
- office365[.]im
- xn--offce365-41a[.]de
- xn--offce365-41a[.]net
- office365s[.]tk

- office365[.]zip
- office365[.]day
- office365a[.]cf
- office365-3[.]de
- office365-9[.]de
- office365-2[.]de
- office365vn[.]vn
- office365pl[.]pl
- o2office365[.]ph
- office365-4[.]de
- msoffice365[.]cc
- office365o[.]net
- office365-7[.]de
- jvoffice365[.]uk
- office365id[.]net
- office365-12[.]de
- office365-21[.]de
- office365-14[.]de
- office365mex[.]cf
- wpsoffice365[.]cn
- office365pc[.]xyz
- weboffice365[.]cn
- office365-18[.]de
- office365-11[.]de
- ofoffice365[.]com
- office365ai[.]com
- office365pro[.]ga
- office365[.]co[.]de
- office365dev[.]ml
- office365-20[.]de
- betoffice365[.]ws
- office365app[.]id
- office365pro[.]tk
- office365-13[.]de
- office365-10[.]de
- weboffice365[.]de
- office365wx[.]xyz

Sample Malicious Office 365 String-Connected Domains

- office365doc[.]cz
- xxxoffice365[.]com
- office365[.]srv[.]br
- office365mail[.]nl
- efaxoffice365[.]com
- office365-axa[.]com
- office365portal[.]cz
- protaloffice365[.]cz
- getoffice365llc[.]com
- owamailoffice365[.]sbs
- msoffice365-teams[.]de
- office365apps[.]support
- office365authpage[.]com
- office365-windows[.]com
- office365microsoft[.]it
- office365supwaytin[.]com
- office3655[.]duckdns[.]org
- login-office365-dhjj[.]in
- microsoft-office365[.]info
- login-office365-accor[.]in
- login-office365-hpblaw[.]in
- privateoffice365secure[.]com
- microsoftsigninoffice365[.]top
- microsoftsigninoffice365[.]info
- loginoffice365-blandgarvey[.]in
- login-office365-ntageneral[.]in
- microsoftsigninoffice365[.]life

Sample RBC Bank String-Connected Domains

- zrbcbank[.]com
- rbcbankpro[.]com
- cs-rbcbank[.]com
- mc-rbcbank[.]com

- cs-rbcbank5[.]com
- cs-rbcbank4[.]com
- cs-rbcbank6[.]com
- cs-rbcbank3[.]com
- cs-rbcbank2[.]com
- kyc-rbcbank[.]com

Sample Malicious RBC Bank String-Connected Domain

- cs-rbcbank2[.]com