BlackCatがRedditを再びハッキング：DNSが明らかにしたこと

目次

要旨

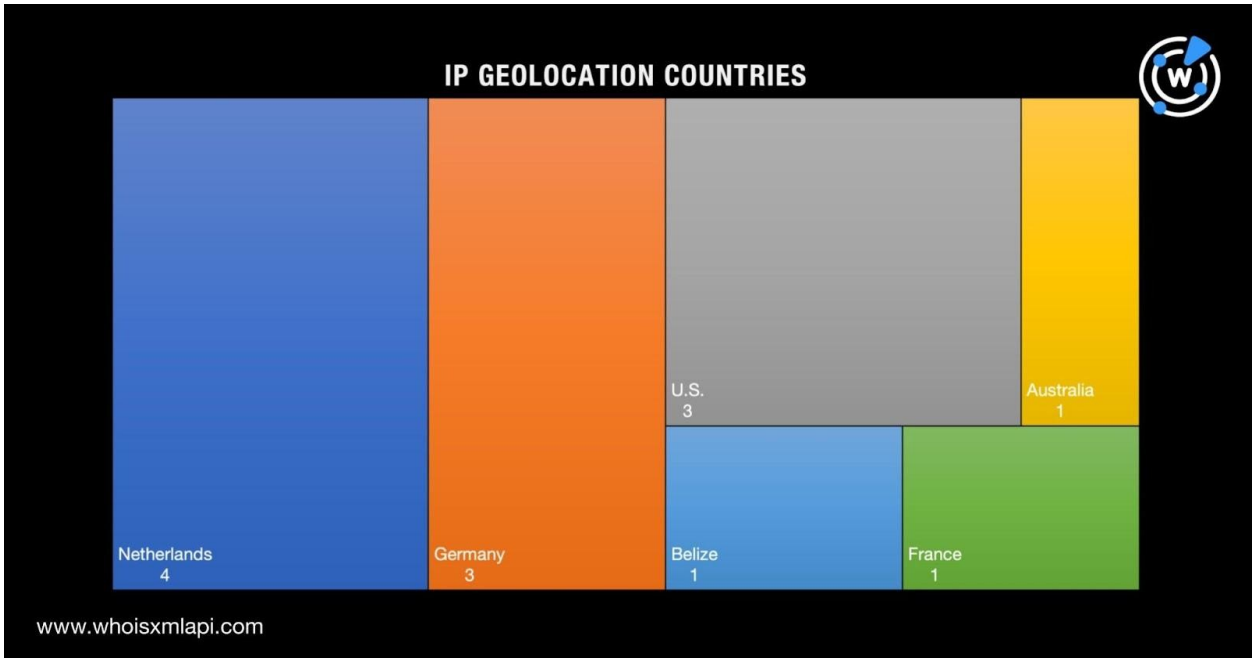
BlackCatのランサムウェアギャングが初めてRedditを攻撃したのは今年2月で、その時は同社の従業員をフィッシングしてネットワークに侵入し、ユーザーデータを窃取しました。ReversingLabsの詳細なレポートによると、最近行われた二度目の攻撃で、犯人たちはRedditのシステムをBlackCatに感染させることに成功し、身代金を支払わなければデータを公開するといって同社を脅迫しました。

WhoisXML APIでは、2023年6月4日に公開された13個のIPアドレスからなるBlackCatのセキュリティ侵害インジケーターの（IoC）リストを拡張するべく、DNSを広範囲に検索しました。その結果、脅威アクターが残した可能性のある以下の痕跡が新たに発見されました。

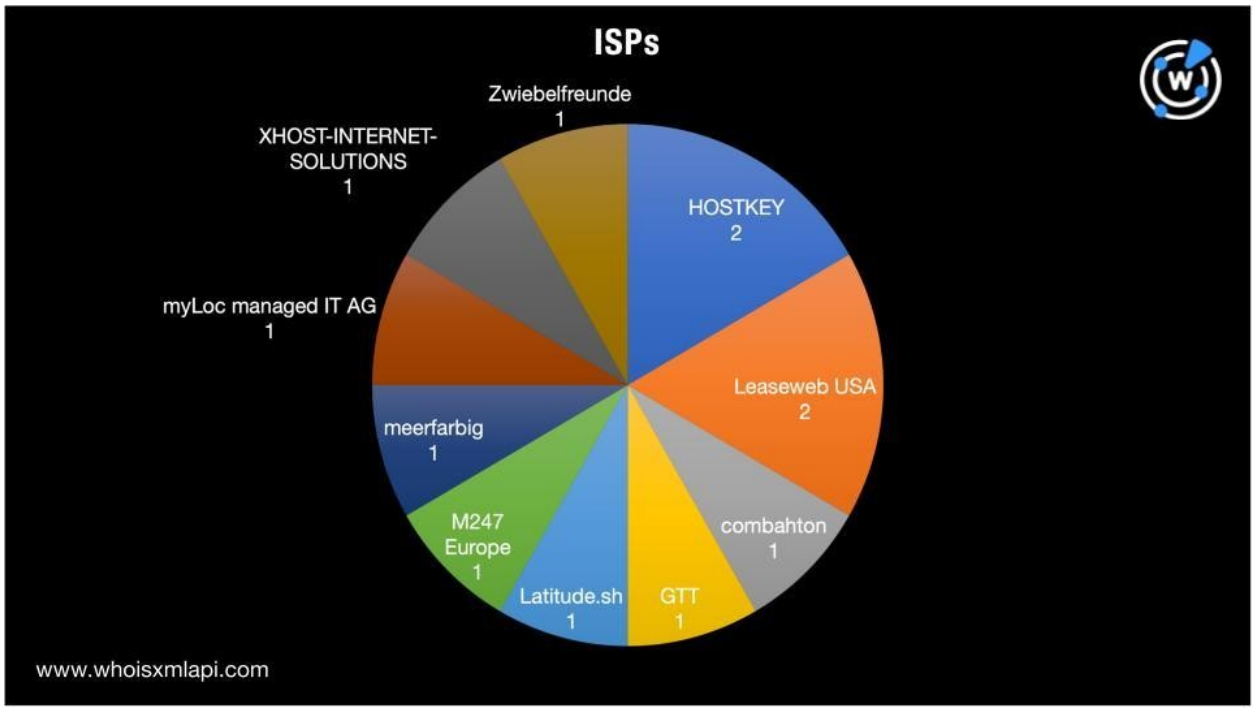
- IoCとして特定された2つの専用IPアドレスでホストされていた3個のドメイン名
- IoCのIPアドレスを使っていたoff365logs[.]onlineというアーティファクトと同様の**office365logs**、**office365**または**off365**という文字列を含むドメイン名が437個。マルウェアの一括チェックにより、そのうち53個は悪意あるドメイン名と判明
- IoCのIPアドレスを使っていたsecure-rbcbank[.]netというドメイン名と同様の**rbcbank**という文字列を含むドメイン名が20個。マルウェアの一括チェックにより、そのうち2個は悪意あるドメイン名と判明

IoCに関する発見

IoCとして特定されたIPアドレスをBulk IP Geolocation Lookupで検索したところ、地理的に6カ国に分散していることがわかりました。最も多くのアドレスが位置していたのはオランダで、4個でした。次いで多かったのはドイツと米国で、それぞれ3個が位置していました。また、オーストラリア、ベリーズ、フランスにそれぞれ1個ありました。



さらに調査を進めると、IoCのIPアドレスを管理するISPが10社特定されました。HOSTKEY、Leaseweb USAおよびM247 Europeが2個のアドレスを、Combahton、GTT、Latitude.sh、Meerfarbig、myLoc managed IT AG、Xhost Internet SolutionsおよびZwiebelfreundeが1個を管理していました。

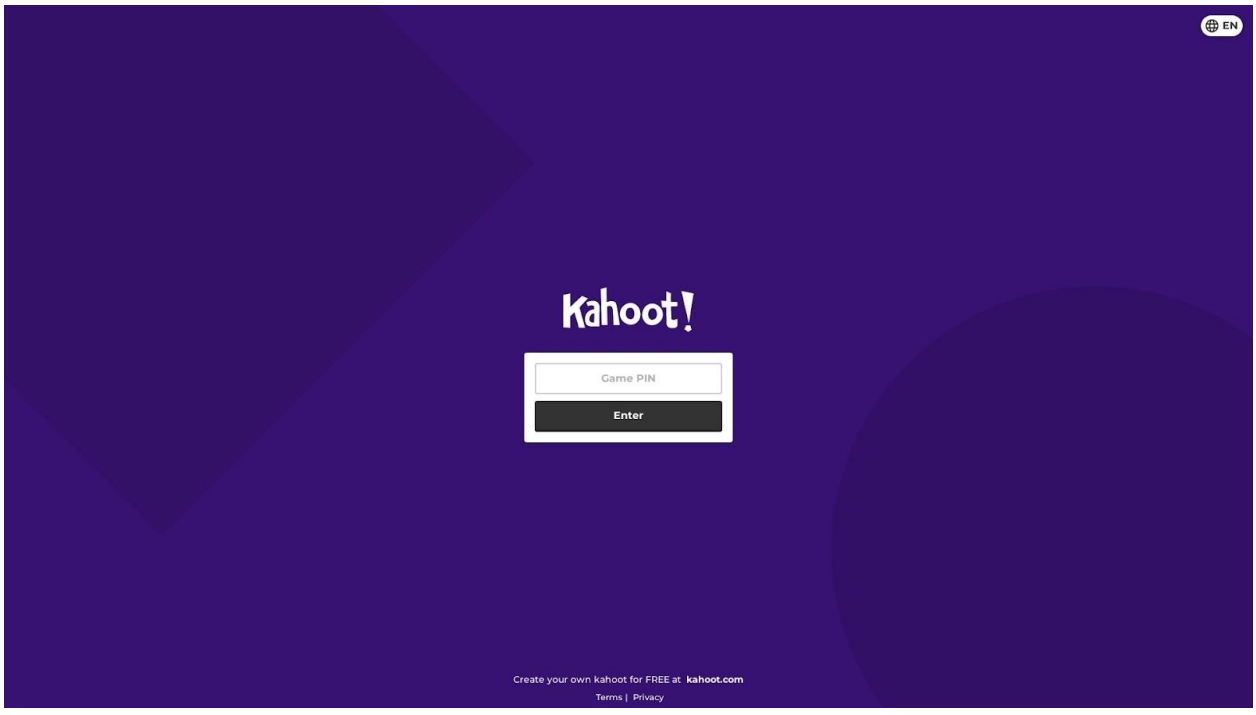


IoCを軸に調査を展開

次にIoCをReverse IP Lookupで検索した結果、2個（89[.]44[.]9[.]243と185[.]220[.]102[.]253）は専用アドレスと確認できました。この2つのIPアドレスは、合わせて3つのドメイン名をホストしており、その3つのドメイン名のうち2つはアクティブなコンテンツをホストし続けていました。また、1つはTorの出口ノードと確認され、残りの2つは見た目からサイバースクワッティングのドメイン名と思われました。

off365logs[.]onlineは、現在パークされているものの、 Microsoft Office 365のページを装っているようでした。しかし、そのWHOISレコードには、microsoft[.]comとの類似性が全くありませんでした。off365logs[.]onlineのレジストラと登録者メールアドレスも、正規のmicrosoft[.]comのそれとは異なっていました。

secure-rbcbank[.]netは、カナダを拠点とするRBC銀行になりすましている可能性があります。上記のサイバースクワッティングドメインと同様、secure-rbcbank[.]netのWHOISレコードも正規のドメイン名であるrbcbank[.]comのそれとは異なっていました。secure-rbcbank[.]net でホストしていたのは、以下の通りKahoot!のログインページです。



secure-rbcbank[.]netのスクリーンショット

off365logs[.]onlineとsecure-rbcbank[.]netのいずれも、今のところ悪意あるドメイン名とはみなされていません。しかし、脅威アクターがこれらを悪用してOffice 365のユーザーやRBC Bankの顧客を攻撃する可能性は十分にあります。なお、secure-rbcbank[.]netのWHOISレコードには、

登録者のメールアドレスが未編集のまま公開されていました。セキュリティ研究者や法執行機関にとっては、調査や捜査を深める上でこのメールアドレスが役立つでしょう。

さらに多くのアーティファクトを収集するため、ブランド名を含み、かつBlackCatランサムウェアの背後にいる脅威アクターに属しているかもしれないドメイン名を探しました。

まず、**office365logs**、**office365**または**off365**という文字列を含み、2023年1月1日以降に新規登録されたドメイン名を当社のDomains & Subdomains Discoveryで検索してみました。その結果、該当するドメイン名が437個特定されました。それらをBulk WHOIS Lookupで調べたところ、登録者のメールアドレスからMicrosoftへの帰属が確認できたドメイン名は3個にとどまりました。また、一括マルウェアチェックを行った結果、それらのうち53個は悪意あるドメイン名と判定されました。その他、以下のことがわかりました。

- 5個のドメイン名（uwu[.]ai、toolforge[.]org、office365[.]com[.]pr、azurestaticapps[.]netおよびoffice365login[.]co[.]il）のレジストラは、Microsoftの正規のドメイン名のレジストラと同じ。しかし、Microsoftが所有していると確認できたドメイン名はそのうち3個（office365[.]com[.]pr, azurestaticapps[.]net, and office365login[.]co[.]il）のみ。
- 260個は今年に入って新規登録されたドメイン名。
- 登録者の国として最も多かったのは米国で、129個のドメイン名が該当。これにカナダ（70個）、中国（12個）が続いた。

次に、上記と同じ期間に登録された**rbcbank**という文字列を含むドメイン名を同様に検索し、19個を特定しました。しかし、そのいずれも公開のドメイン名情報からRBC Bankへの帰属を確認できませんでした。また、一括マルウェアチェックにより、それらのうち2個は悪意あるドメイン名と確認されました。加えて、以下が判明しました。

- RBC Bank関連の文字列を含むドメイン名のうち、rbcbank[.]com（RBC Bankの正規のドメイン名）と同じレジストラを使っていたものはなかった。
- 18個は今年に入って新規登録されたドメイン名。
- 登録者の国として最も多かったのは米国で、9個のドメイン名が該当。その他、カナダが3個、オランダとセーシェルが各2個、ウズベキスタンが1個。

—

今回、BlackCatによる最新のRedditへの攻撃を精査した結果、IoCと同じIPアドレスを共有していたり、共通の文字列を含んでいたりする未公開のアーティファクトが460個見つかりました。

新たに発見されたドメイン名のうち合計55個は、調査の時点でマルウェアチェッカーによって悪意があるものと判定されたことから、すでにサイバー攻撃やフィッシングキャンペーンで使用された可能性があります。そして、これらのアーティファクトの大部分は、特にOffice 365ユーザーやRBC銀行の顧客を標的とした他の攻撃のために悪用されやすいと思われます。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IoCとして特定されたIPアドレス

- 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

IoCとされた専用IPアドレスでホストされていたドメイン名の例

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

Office 365関連の文字列を含むドメイン名の例

- 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

Office 365関連の文字列を含む悪意あるドメイン名の例

- 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

RBC Bankという文字列を含むドメイン名の例

- 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

RBC Bankという文字列を含む悪意あるドメイン名の例

- cs-rbcbank2[.]com