# カーディングは今も盛況：DNSインテリジェンスで判明

## 目次


1. 要旨
2. 付録：アーティファクトとIoCの例


## 要旨


カーディングは1980年代から存在していましたが、今では経験の浅いサイバー犯罪者でもキャンペーンを展開できるまでに進化しています。どうやって？彼らは最近ウェブに溢れているカーディング・フォーラムを利用するのです。

当社のセキュリティ研究者であるDancho Danchevは最近、カーダーのものと思われる220個のメールアドレスを収集しました。そこで、WhoisXML APIの研究チームがこのほど、それらのセキュリティ侵害インジケーター（IoC）リストをもとにDNSを調査し、関連性が疑われる以下のアーティファクトを特定しました：

- 共通のメールアドレスを使用している865個のドメイン名。マルウェアの一括チェックにより、そのうち157個に悪意があることが判明
- 共通のメールアドレスを使用しているドメイン名が解決した361個のIPアドレス
- 共通のIPアドレスを使っているドメイン名489個。マルウェアの一括チェックにより、そのうち2個には悪意があることが判明

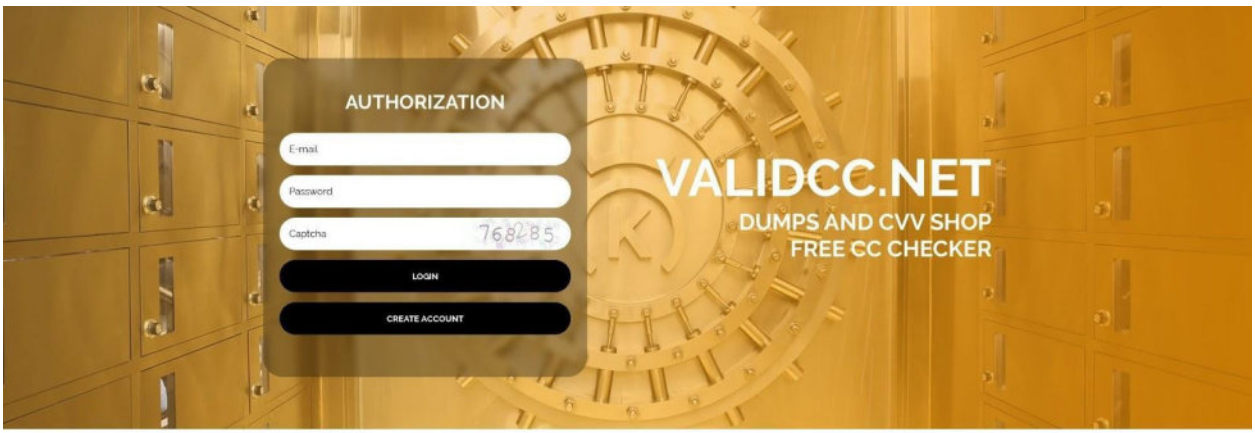

### カーダーのメールアドレスの詳細

まず、IoCと特定された220個のメールアドレスに対してReverse WHOISのAdvanced Searchを使ったWHOIS過去データの検索を行いました。その結果、220個のメールアドレスのうち97個が、最近72,197個のドメイン名の登録に使用されたことがわかりました。

今回の調査では、50個以下のドメイン名の登録に使用された76個のメールアドレスに対象を絞りました。これにより、865個のドメイン名がサンプルとして残りました。

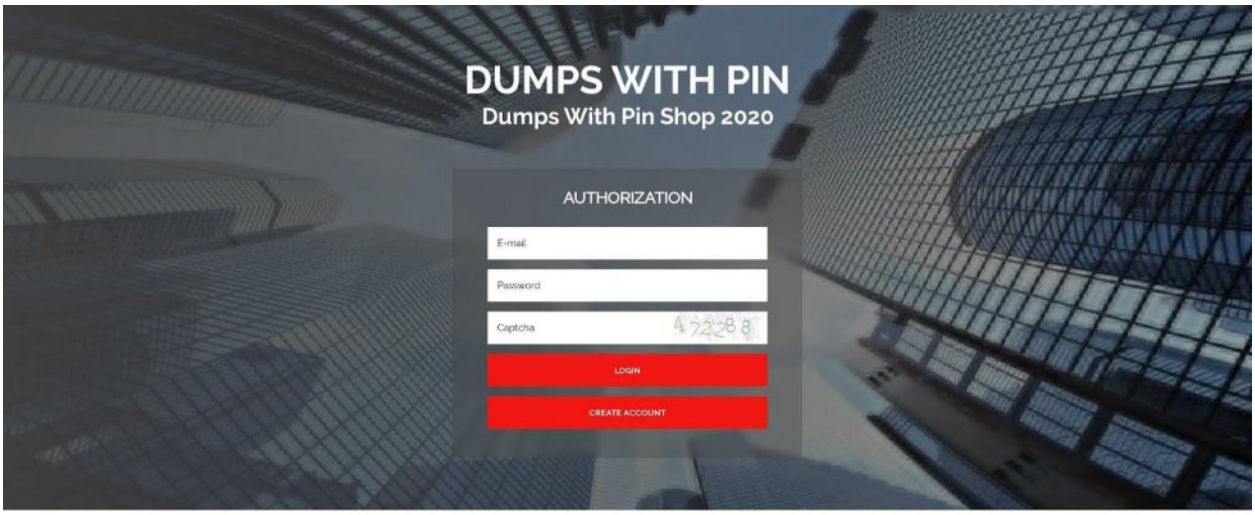
マルウェアの一括チェックにかけたところ、そのうち157個が悪意あるドメイン名であることが

わかりました。そして、そのうち75個が依然としてアクティブな状態でした。49個は有効なページに誘導されましたが、Screenshot Lookupの結果から、そのうち44のサイトはカーディング関連と判明しました。また、21個はパーキングページに、5個は空白のページに繋がりました。以下はカーディング関連ページのスクリーンショットの例です。





**共通のメールアドレスを使用している悪意あるドメイン名「domain 2card[.]su」のスクリーンショット**





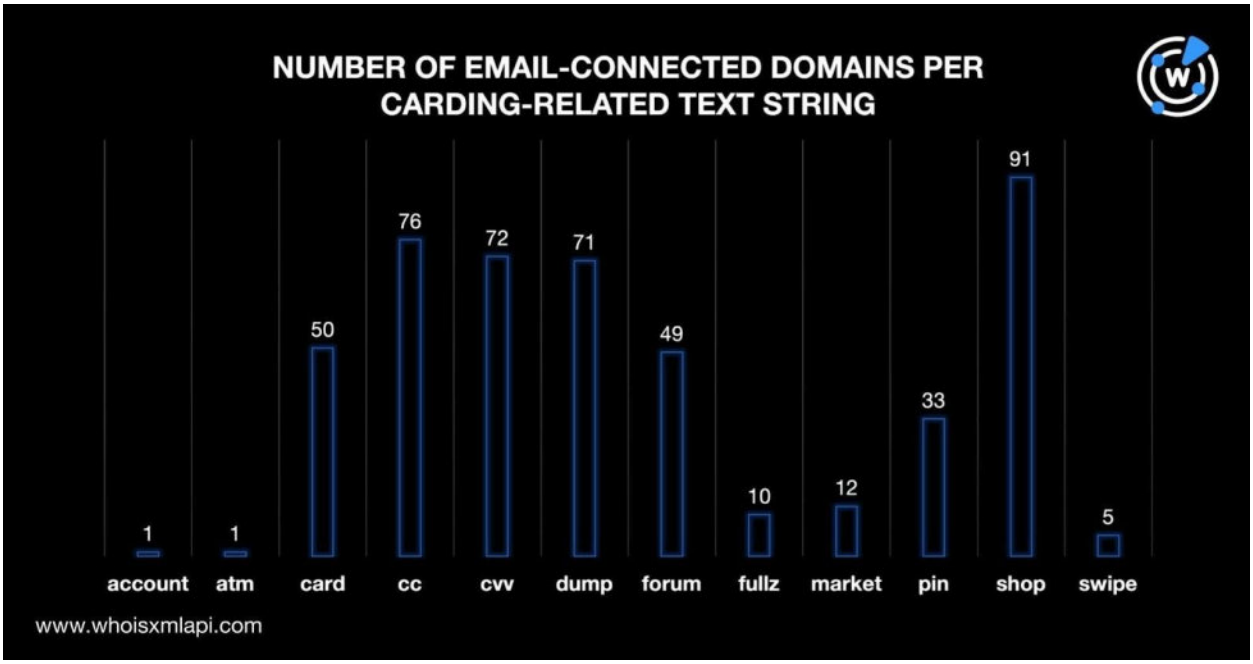
**共通のメールアドレスを使用している悪意あるドメイン名「approvedcc[.]su」のスクリーンショット**


**共通のメールアドレスを使用している悪意あるドメイン名**
**「best-cvvshop[.]com」のスクリーンショット**

共通のメールアドレスを使っている別のドメイン名からは、カーディングのフォーラムに誘導されました。

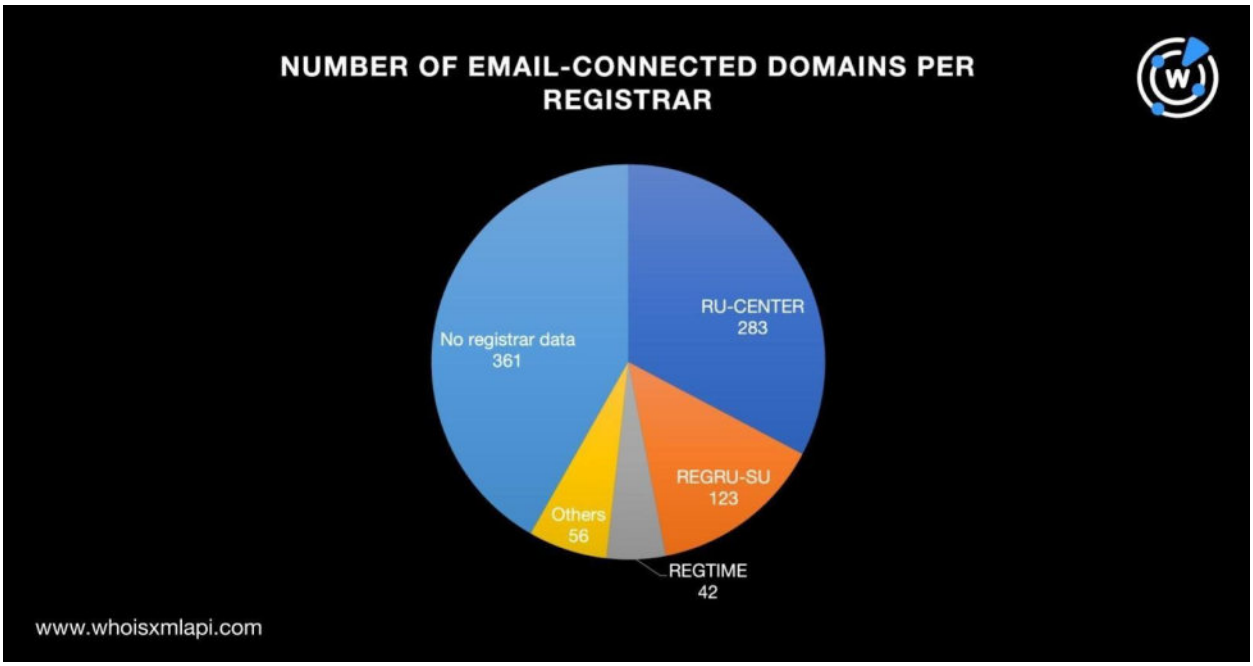

**共通のメールアドレスを使用している悪意あるドメイン名**
**「cardingforum[.]cx」のスクリーンショット**

また、当社の分析により、カーディングに関連する12種類の文字列をドメイン名の中に見出すことができました。1個のドメイン名の中に複数種類のそうした文字列が含まれている場合もあります。以下は、カーディング関連の文字列ごとに、その文字列が含まれており、かつ共通のメールアドレスを使用しているドメイン名の数を示しています。

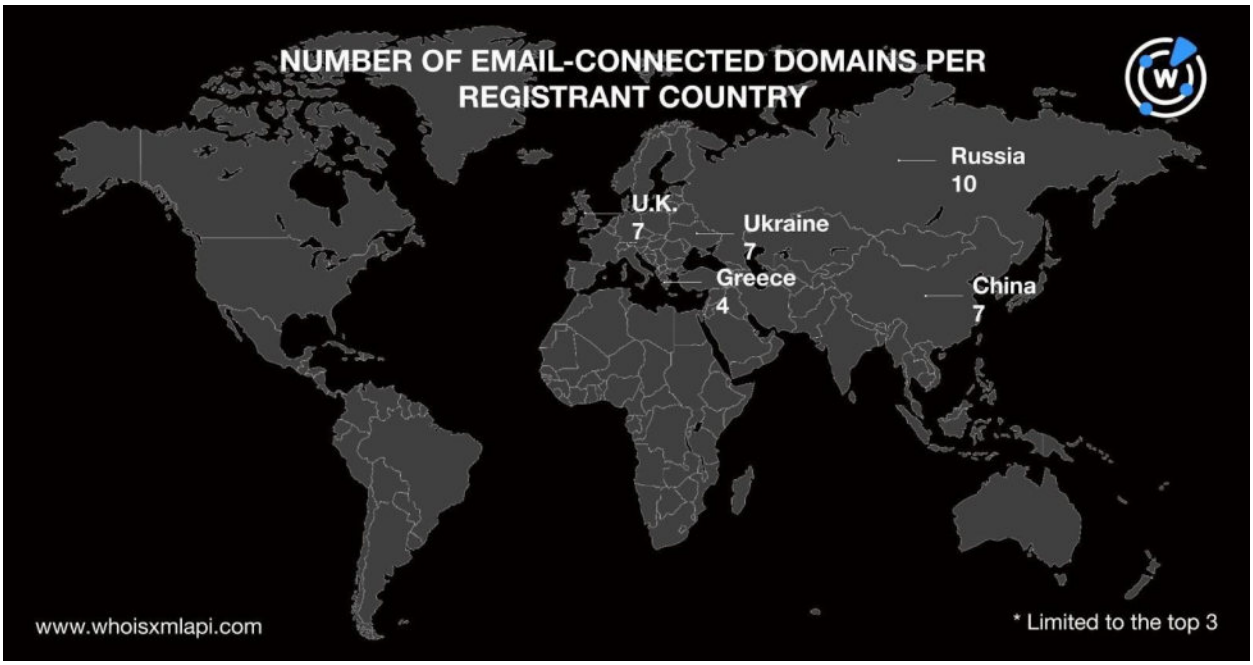



**Shop**が最も多く、**cc**（「credit card」の略）そして**cvv**がそれに続きます。 なお、これらの数字には、今回我々が確認したスペルミスのバリエーションを含むドメイン名は含まれていません。

次に、共通のメールアドレスを使用している865個のドメイン名をBulk WHOIS Lookupにかけました。その結果、管理レジストラのトップ3がRU-CENTER（283ドメイン）、REGRU-SU（123ドメイン）およびREGTIME（42ドメイン）であることを確認しました。361個のドメイン名はレジストラデータを公開していませんでした。そして、残りの56個は他の20社のレジストラに分散していました。



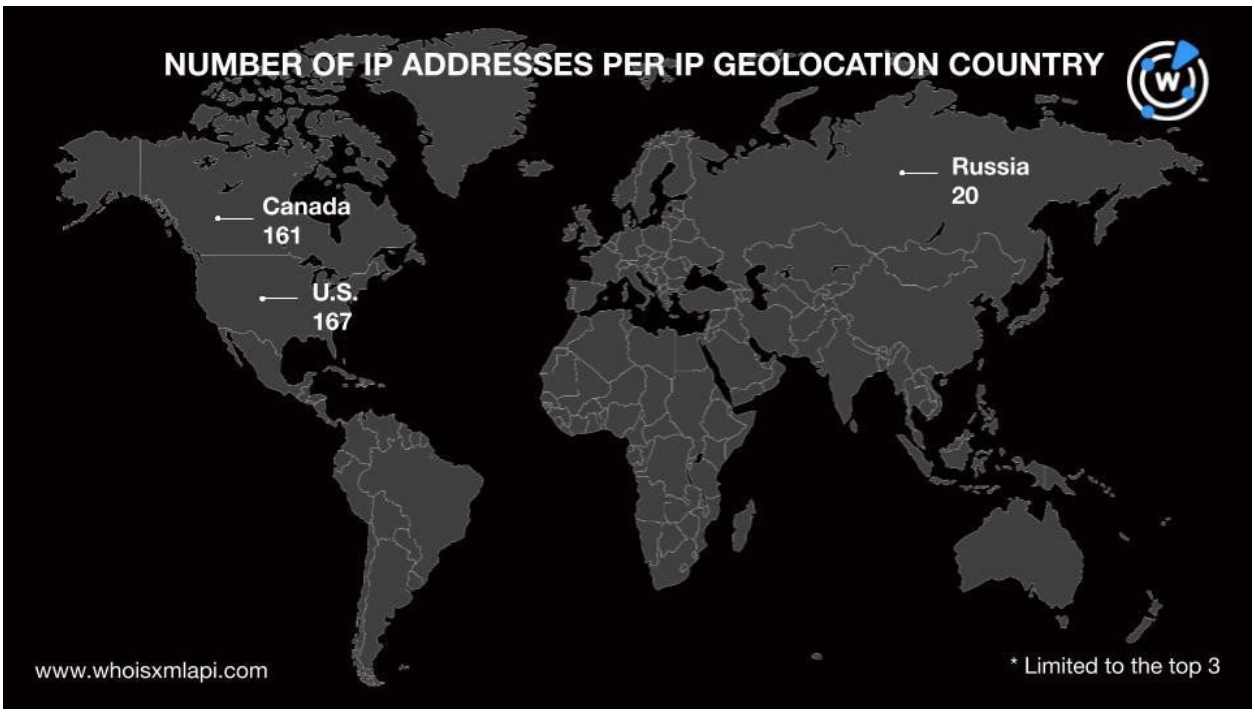

最も多くの登録者が位置していた国はロシア（10ドメイン）でした。次いで多かったのは中国、ウクライナ、英国（各7ドメイン）でした。共通のメールアドレスを使用していた823個のドメイン名は登録者の国のデータを公開していませんでしたが、残りの7個は別の4カ国で登録されていました。



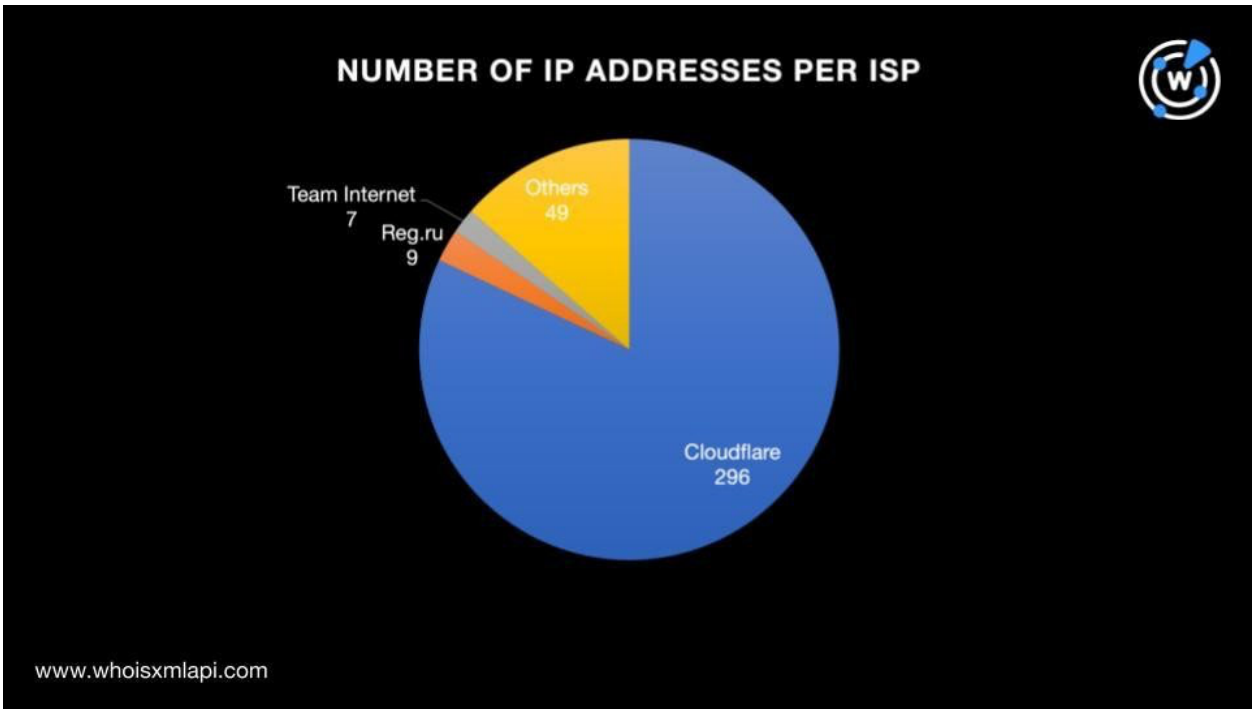
関連している可能性のあるアーティファクトをさらに収集するため、共通のメールアドレスを使っている865個のドメイン名に対してDNS Lookupを実行しました。その結果、602個は有効なIPアドレスに名前解決しました。重複を取り除いた結果、361個のIPアドレス（211個のIPv4アドレスと150個のIPv6アドレス）が残りました。

## IPアドレスの詳細分析

その361個のIPアドレスをBulk IP Geolocation Lookupで調べたところ、IPアドレスのジオロケーションのトップ3は米国（167アドレス）、カナダ（161アドレス）、ロシア（20アドレス）となりました。残りの13アドレスは他の6カ国に分散していました。



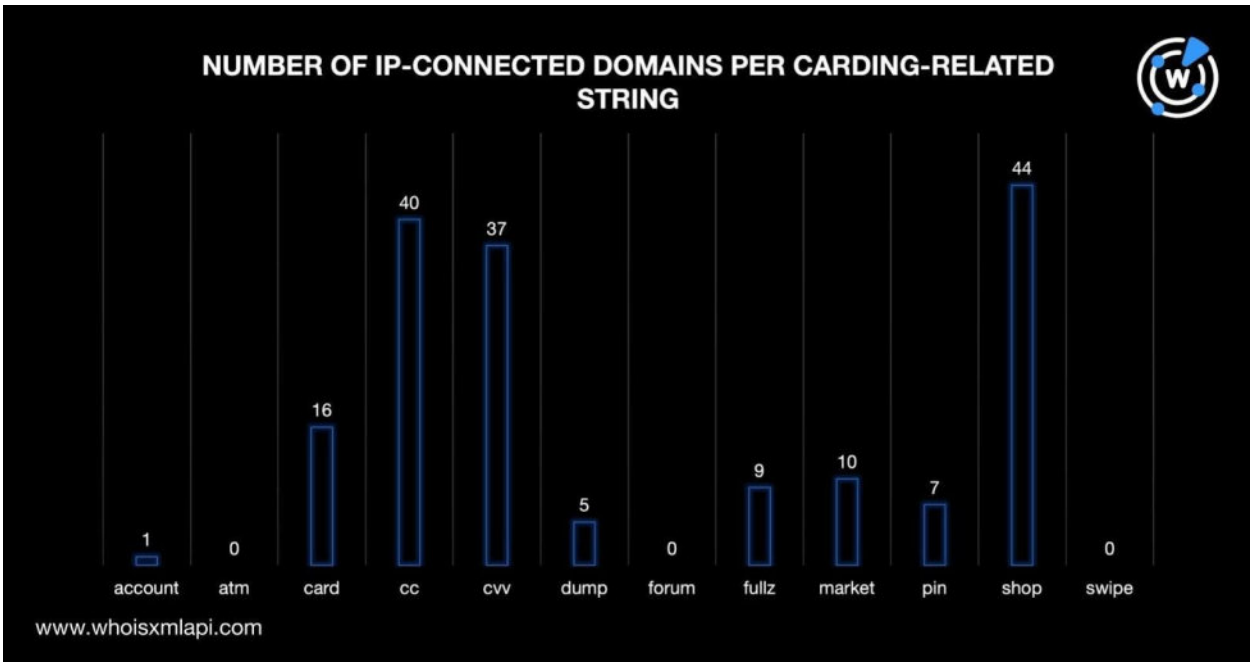

また、361個のIPアドレスは、Cloudflare（296個）、Reg.ru（9個）、Team Internet（7個）を筆頭に、34の管理ISPに分散していることがわかりました。残りの49アドレスは他の31のISPに分散していました。




次に、分析の範囲を211個のIPv4アドレスに絞り込みました。これらのアドレスに対してReverse IP Lookupを実行した結果、192個が共用、14個がおそらく専用、5個が現在ドメイン名をホストしていないアドレスであることが判明しました。そこで、脅威と密接に関連するアーティファクトを確実に取得するため、調査のサンプルをさらに専用と思われるIPアドレスのみに限定しました。

その14個のIPアドレスは531個のドメイン名をホストしていました。その531個から重複や共通のメールアドレスを使っているとして特定されたドメイン名を取り除いた後、共通のIPアドレスを使用しているドメイン名が489個残りました。このドメイン名に対してマルウェアの一括チェックを行った結果、2個のドメイン名が悪意あるものと判明しました。その両方ともオンラインのままでしたが、いずれもカーディングとは無関係のようでした。

共通のメールアドレスを使用しているドメイン名について行なった調査と同様に、共通のIPアドレスを使っている211個のドメイン名についても、12種類のカーディング関連文字列を使っているものがいくつあるかを調べました。結果の内訳は以下の通りです。




共通のIPアドレスを使用しているドメイン名の場合も**shop**がトップで、これに**cc**、**cvv**が続きました。共通のメールアドレスを使用しているドメイン名について調査した結果と整合しています。

—

カーディングのIoCとして特定された220個のメールアドレスをDNSで徹底的に調査した結果、関連しているドメイン名とIPアドレスが合計1,715個検出されました。それらをマルウェアチェックにかけたところ、159個は悪意あるアーティファクトに分類されました。

***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として特定されたメールアドレス

- 0daysu@mail[.]ru
- 10xmoney[.]site@regprivate[.]ru

- 1254189890@qq[.]com
- 3263718675@qq[.]com
- 3463929680@qq[.]com
- 363325361@qq[.]com
- abbysilva@tutanota[.]com
- abdullaev09@gmail[.]com
- abuse@carders[.]su
- abuse@dronislaw[.]com
- admin@1CHEAPEST[.]SU
- admin@2PAC[.]SU
- admin@BACKSTAB[.]SU
- admin@BIG-DUMPS[.]RU
- admin@bpcsquad[.]com
- admin@dumplogs[.]com
- admin@n1name[.]su
- admin@trusted[.]su
- afanasev[.]p@gmail[.]com
- ahujanaman5@gmail[.]com
- akfs@list[.]ru
- akfsd@list[.]ru
- alexlopez88@protonmail[.]com
- apnapakforum@gmail[.]com
- apvpsedo@gmail[.]com
- aqerhett@rambler[.]ru
- ARGJENTCRX@GMAIL[.]COM
- artem[.]v[.]ponomarev@gmail[.]com
- asentli2@gmail[.]com
- auction@nic[.]ru
- babicheva[.]roksana@yandex[.]com
- baenko-marina@bk[.]ru
- bazzamin[.]sofia@yandex[.]com
- bersenevskaya@gmail[.]com
- bibip777@protonmail[.]com
- bosnianw00rm@gmail[.]com
- brian@brianarndt[.]com
- brodieglennyaus@gmail[.]com
- bunch[.]randy@yandex[.]com
- buyers[.]ticket@gmail[.]com
- cardchinaunionpay@gmail[.]com
- carder[.]forum@yahoo[.]com
- carding-world[.]com@whoisproxy[.]ru
- CardMafia@yandex[.]com
- cashorika@gmail[.]com
- cgqltd@yahoo[.]com
- chen_light@outlook[.]com
- clientvps@mail[.]ru
- contactprivatedomain@yandex[.]com
- crdpro@rambler[.]ru
- cvvme@iampablo[.]eu
- dbinar@mail[.]ru
- deonprice123@gmail[.]com
- desirabletizb@gmail[.]com
- devilteam@devilteam[.]su
- dnsmaster@hostland[.]ru
- domain@esc0bar[.]net
- domain@iampablo[.]eu
- domain@paysafehost[.]com
- domains@marcaria[.]com
- domains@marshall[.]co
- domenikivareniki@rambler[.]ru
- domenregru@proton[.]me
- domentr3@rambler[.]ru
- domikdddn@rambler[.]ru
- domindomenov2@rambler[.]ru
- dyachkovegorovvj@mail[.]ru
- eleoxise@gmail[.]com
- fabio-leitao@yandex[.]com
- ferum@eurodns[.]me
- ferum@iampablo[.]eu
- florin[.]grigore1@outlook[.]com
- forumcarder@9[.]cn
- fretsellhandroothenab823@rambler[.]ru
- ga[.]special@mail[.]ru
- gaqw9lneita@rambler[.]ru
- gennaro@encrypt[.]su
- gergk34@mail[.]ru
- god[.]isreal@yandex[.]com

- gogoanimetv@gmail[.]com
- goodcvv[.]su@allperson[.]ru
- greg2022@mail[.]ru
- gullashop@85mail[.]com
- handbags@foxmail[.]com
- holgen89@mail[.]ru
- hqcc[.]su@allperson[.]ru
- huges98@protonmail[.]com
- icalls@126[.]com
- ifeanyichukwufrancis50@gmail[.]com
- igor[.]tckalitch@yandex[.]ru
- imasifrasool00@gmail[.]com
- info@domcollect[.]com
- info@lagomcloud[.]net
- info@netengi[.]com
- info@she-and-style[.]ru
- inserel@mail[.]ru
- ivanovsergeidomen@rambler[.]ru
- james@encrypt[.]su
- jamie[.]reed216@gmail[.]com
- janeverno@gmail[.]com
- javirock906@gmail[.]com
- john@encrypt[.]su
- justvalid@outlook[.]com
- KingsCard@admin[.]com
- kissanime[.]es@gmail[.]com
- lapaevreshaet@gmail[.]com
- laurene6fh@rambler[.]ru
- laza[.]cool@yandex[.]com
- legion[.]web@mail[.]ua
- leninmixail@mail[.]ru
- lermontov5454@mail[.]ru
- liladilicont@lenta[.]ru
- long1765@163[.]com
- long1765@gmail[.]com
- Madarano1@hotmail[.]com
- magnetj47@gmail[.]com
- mailqueries@inbox[.]ru
- makaricev@bk[.]ru
- maratistrov@rambler[.]ru
- marketingoffdirekt@yandex[.]ru
- mayland@korea[.]com
- MIKE@ADUTOPIA[.]COM
- mike@emarketology[.]com
- milanmarinkovic83@mail[.]ruv
- mildred[.]noel@yandex[.]com
- MILENRADUMILO@GMAIL[.]COM
- mollyscarlette@aol[.]com
- mrccroom@sigaint[.]org
- mrs[.]akimanna@yandex[.]ru
- muqiang@126[.]com
- myfreemail@ya[.]ru
- mypersonalshinjiru@gmail[.]com
- nbuy-domaine@mail[.]ru
- ner@mmm[.]mp
- nesternko43@mail[.]ru
- newland003@gmail[.]com
- noreply@r01[.]ru
- norman@encrypt[.]su
- offshore7x@ru[.]ru
- olddealer[.]s@gmail[.]com
- opabook@hotmail[.]com
- optbaseop@mail[.]ru
- orbibahuwani356@rambler[.]ru
- outsidecharleston@gmail[.]com
- owner@fe-acc18[.]su
- owner@fe-acc19[.]su
- perst3355@mail[.]ru
- pinoymovies[.]su@gmail[.]com
- planetary100@hotmail[.]com
- polanrm@gmail[.]com
- prenok44@online[.]ua
- privacy@1and1[.]com
- privacy@dynadot[.]com
- privacy@fortguard[.]su
- private[.]person1982@ya[.]ru
- prokatyperry@gmail[.]com
- qaisrani4051@gmail[.]com
- qweiggi@gmail[.]com

- r01su1@rambler[.]ru
- ragged[.]bag@gmail[.]com
- ramenskdom@rambler[.]ru
- randy@encrypt[.]su
- ravibansal24@gmail[.]com
- rawixidawax@hotmail[.]com
- regrucoms@proton[.]me
- regsu1@rambler[.]ru
- regsuion2@rambler[.]ru
- resorepesu@lenta[.]ru
- ristmasc@gmail[.]com
- robertjohnson5268@outlook[.]com
- roksana@encrypt[.]su
- roksana@iampablo[.]eu
- RoksanaBitcoin@yandex[.]com
- romanova_mashag4549@rambler[.]ru
- rscp888@gmail[.]com
- ruslanabrykova@rambler[.]ru
- sale@domainsale[.]io
- sasuketeam9@hotmail[.]com
- savinevgeniyahdl@mail[.]ru
- sergey@vishnyakov[.]org
- smirnov[.]andrey70@mail[.]ru
- snoozopreswilighdres793@rambler[.]ru
- sstrakatos@yahoo[.]com
- stilon88@mail[.]ru
- stolychevlev01@rambler[.]ru
- studio1974@gmail[.]com
- subwaybham@gmail[.]com
- support@DropCatch[.]com
- sysseo09@gmail[.]com
- t2cvv@dnsname[.]info
- takeeasy1@yahoo[.]com
- teifilpeodifulor670@rambler[.]ru
- tereston@mail[.]ru
- thedumps@evermail[.]org
- thompsonl@gtlaw[.]com
- tima96-2009@mail[.]ru
- titovvitaliysvvq@mail[.]ru
- tonystuff[.]su@rambler[.]ru
- tores4477@mail[.]ru
- try2buy007@gmail[.]com
- ttimeinfo1@gmail[.]com
- uasservices[.]ru@gmail[.]com
- ulrich@encrypt[.]su
- usama[.]jamil@outlook[.]com
- valentina@whoisprivacy[.]website
- validdumps[.]su@allperson[.]ru
- vermon4433@mail[.]ru
- vhungcc[.]kd@gmail[.]com
- viber1919@gmail[.]com
- viktrov@tutanota[.]com
- wiktrov@yandex[.]ru
- yngert@mail[.]ru
- yonabaruyoshi@hotmail[.]com
- ywgsky@163[.]com
- zanebilly30@gmail[.]com
- zaxarovserg@online[.]ua
- zubairbaloch350@gmail[.]com

## 共通のメールアドレスを使用していたドメイン名の例

- 101-dumps-with-pin-atm-nickstuff[.]su
- 1337x[.]su
- 148[.]su
- 18sgorg[.]com
- 1kinox[.]su
- 2-ch[.]su
- 257[.]su
- 2asi[.]net
- 2card[.]su
- 2nsk[.]net
- 2pac[.]cc

- 2pac[.]su
- 2r4b[.]biz
- 2r4b[.]net
- 2rich4b[.]com
- 2rich4bitch[.]biz
- 2rich4bitch[.]com
- 3839000[.]com
- 4airlinetickets[.]com
- 4anime[.]su
- 4banquets[.]com
- 4barbecue[.]com
- 4baseballcards[.]com
- 4chan[.]jp
- 4equipmentleasing[.]com
- 4freecellphones[.]com
- 4freewebsite[.]com
- 4healthclubs[.]com
- 4mailorder[.]com
- 4onlinetickets[.]com
- 4springwater[.]com
- 4usedcarparts[.]com
- 5191[.]org[.]cn
- 525554[.]net
- 69nombres[.]net
- 786centre[.]net
- 850score[.]su
- 88ttyule[.]com
- 919604[.]net
- 948w[.]net
- 9anime[.]cm
- 9goalstv[.]com
- aab-law[.]net
- aamee[.]net
- abags[.]su
- abdulhafiz[.]net
- adsensebancheck[.]net
- aescentral[.]net
- afhil[.]net
- agnimedia[.]net
- ahfloors[.]net
- alamooil[.]net
- alcatraz[.]su
- aljur[.]net
- allchan[.]su
- allworldcard[.]net
- aloevera[.]su
- altenen[.]su
- altenens[.]su
- alugueres[.]net
- analit[.]su
- anime-freak[.]su
- animefenix[.]su
- animefire[.]su
- animeflv[.]su
- animeheaven[.]su
- animekisa[.]su
- animepahe[.]su
- animesuge[.]su
- animetake[.]biz
- animetake[.]su
- animeunity[.]su
- aniwave[.]net
- anoboy[.]su
- anon-sh0p[.]com
- apniclub[.]xyz
- approved-shop[.]su
- approved-xxx[.]su
- approved[.]su
- approvedcc[.]su
- aramatr[.]net
- arewq[.]net
- ark-heating[.]com
- asentli[.]com[.]ua
- askmesmile[.]com
- asmsport[.]su
- astra-shop[.]su
- astratruck[.]su
- ati-internazionale[.]com
- auction-nic[.]ru
- babli[.]su

- bags7[.]su
- bagsall[.]su
- banzaj[.]su
- belli-group[.]online
- best-cvvshop[.]com
- bestbins[.]su
- bestdumps[.]su
- bestswipe[.]su
- besttraffic[.]mobi

## 共通のメールアドレスを使用していた悪意あるドメイン名の例

- 2card[.]su
- 2pac[.]cc
- 2pac[.]su
- 2r4b[.]net
- 4anime[.]su
- alcatraz[.]su
- anime-freak[.]su
- animefire[.]su
- aniwave[.]net
- approved[.]su
- approvedcc[.]su
- babli[.]su
- best-cvvshop[.]com
- bestbins[.]su
- bestdumps[.]su
- bezlica-forum[.]com
- bezlicaforum[.]com
- bigfat[.]su
- binbase[.]su
- binswork[.]su
- black-pirat[.]com
- blackservice[.]su
- blackspigot[.]su
- briansdump[.]su
- buycvv2[.]su
- buycvvdumps[.]com
- buycvvonline[.]su
- buydeus[.]su
- buydmp[.]su
- bvcc[.]su
- c4c[.]su
- candywendy69[.]net
- card-dumps[.]su
- carder00[.]com
- carderscave[.]su
- carding-planet[.]su
- carding-world[.]com
- cardingforum[.]cx
- cardingpro[.]su
- cardingwith[.]com
- cardrock[.]su
- cards101[.]net
- cardshop[.]su
- cardstorm[.]su
- cc-cvv[.]su
- cc-dumps-free[.]su
- cc-stock[.]su
- ccbase[.]su
- ccbox[.]su
- ccdumps[.]su

## 関連IPアドレス

- 104[.]247[.]82[.]50
- 104[.]21[.]10[.]14
- 172[.]67[.]131[.]57
- 104[.]247[.]81[.]54
- 188[.]40[.]131[.]149
- 185[.]154[.]192[.]74
- 104[.]247[.]81[.]53
- 77[.]232[.]38[.]222
- 154[.]55[.]74[.]53
- 170[.]106[.]48[.]231

- 104[.]247[.]82[.]51
- 103[.]224[.]182[.]253
- 64[.]190[.]63[.]111
- 172[.]67[.]171[.]18
- 104[.]21[.]71[.]165
- 104[.]247[.]82[.]52
- 95[.]214[.]26[.]23
- 194[.]67[.]71[.]186
- 172[.]67[.]213[.]219
- 104[.]21[.]50[.]238
- 104[.]247[.]81[.]51
- 104[.]21[.]62[.]247
- 172[.]67[.]141[.]56
- 104[.]21[.]21[.]123
- 172[.]67[.]198[.]156
- 104[.]21[.]26[.]123
- 172[.]67[.]136[.]64
- 104[.]247[.]81[.]50
- 104[.]21[.]95[.]127
- 172[.]67[.]144[.]245
- 172[.]67[.]149[.]106
- 104[.]21[.]29[.]152
- 104[.]21[.]1[.]109
- 172[.]67[.]129[.]44
- 172[.]67[.]159[.]242
- 104[.]21[.]49[.]69
- 81[.]19[.]140[.]124
- 172[.]67[.]177[.]149
- 104[.]21[.]51[.]84
- 104[.]21[.]0[.]83
- 172[.]67[.]150[.]178
- 178[.]210[.]92[.]7
- 104[.]21[.]47[.]85
- 172[.]67[.]145[.]250
- 31[.]177[.]76[.]32
- 31[.]177[.]80[.]32
- 104[.]247[.]81[.]52
- 91[.]234[.]32[.]16
- 104[.]247[.]82[.]54
- 172[.]67[.]199[.]191

## 共通のIPアドレスを使用していたドメイン名の例

- 100bonus[.]ru
- aaaepoxy[.]com
- aadharenterprise[.]com
- aadyatechsolutions[.]com
- abogadoscolombia[.]com[.]co
- afa1983[.]com
- agamparivahan[.]com
- agondaparadise[.]co[.]in
- ahorros-sucredito[.]com
- aincaltda[.]com
- aivlm-icblr[.]in
- akashenterprises[.]com
- allworld-cc[.]su
- allworld-store[.]ru
- anjanifusion[.]ae
- aoneluxurypg[.]com
- apollobrights[.]com
- appaqua[.]com
- approvedbazar-store[.]ru
- approvedccsu[.]ru
- architektur-hb[.]de
- archpromotions[.]co[.]in
- artforheartbangalore[.]com
- assorti[.]in
- ausowa[.]de
- autoindex[.]in
- badenhost[.]de
- badenregio[.]de
- balakrishnagold[.]com
- banalitybiz[.]ru
- bangalore-cabs[.]com
- barandok[.]ru
- bazar-approved[.]ru
- bazar-vclub[.]ru

- bazar-vclub[.]su
- bazarsvclubs[.]ru
- bazarvclub[.]ru
- beautrix[.]co[.]uk
- berer[.]net
- bilaushopme[.]ru
- binssu[.]ru
- biosas[.]net
- bjmusicalworks[.]com
- bl-open[.]com
- blackforest-sc[.]com
- blekcheckerga[.]ru
- blueriveruae[.]com
- bookmaker10[.]com
- bookmarks[.]com[.]ua
- briansclubcm[.]ru

### 共通のIPアドレスを使用していた悪意あるドメイン名の例

- aincaltda[.]com