DNSでNevadaランサムウェアの足跡を辿る

目次

要旨

Resecurityの脅威リサーチャーが先般、アンダーグラウンドコミュニティのRAMPで「Nevada」という新しいランサムウェアが販売されているのを見つけました。同社の分析によれば、Nevadaは2023年1月だけで複数回のアップグレードされており、主にダークウェブのRansomware-as-a-service（RaaS）モデルを介して非英語圏の脅威アクターの手に渡り、WindowsとLinuxのユーザーを苦しめているといいます。

WhoisXML APIはこのほど、AlienVault OTXが作成したセキュリティ侵害インジケーター（IoC）のリスト（下表の通り）をもとに、Nevadaの足跡をDNSで調べました。

IPアドレス	ドメイン名
• 1[.]23[.]82[.]72 • 106[.]177[.]224[.]34 • 138[.]112[.]25[.]25 • 2[.]12[.]51[.]56 • 21[.]15[.]46[.]55 • 35[.]3[.]46[.]245 • 36[.]75[.]75[.]75	• 2fgithub[.]com • click[.]compare • click[.]contact • click[.]discover • click[.]open • click[.]org • click[.]talk • click[.]zero • continue[.]email • github[.]co • repository[.]click • signup[.]team • submit[.]org

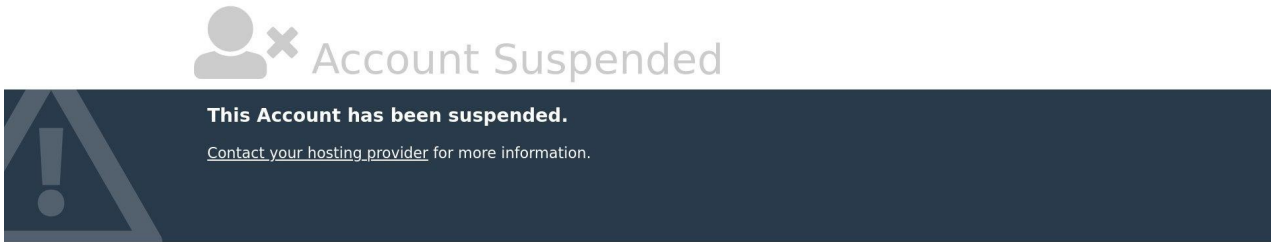
そして、調査の結果、以下を新たに発見しました。

- IoCのドメイン名が名前解決した8個のIPアドレス
- IoCドメイン名1個の過去のWHOISレコードから、編集されていない登録者メールアドレス1個
- 1個のIoCの登録者メールアドレスと同じメールアドレスを使っていた79個のドメイン名。そのうち1個は悪意あるドメイン名と確認
- 一部のIoCと同じIPアドレスを共用していた1,178個のドメイン名。そのうち1個はマルウェアホストと判明
- ***github***、***click***、 ***continue***、***repository***、***signup***および***submit***という文字列を含む2,098個のドメイン名。そのうち3個は悪意あるドメイン名と確認

Nevadaランサムウェアの足跡を解明

まず13個のドメインIoCをDNS lookupsで検索したところ、IoCリストに含まれていない8個のIPアドレスが新たに見つかりました。それらをIoCリストに含まれている7個のIPアドレスとともにReverse IP lookupにかけた結果、4個は専用ホスト、別の4個は共用ホストであることがわかりました。残りの7個はドメイン名に名前解決しませんでした。

このReverse IP lookupでは、1,178個のドメイン名も新たに検出されました。そのうち、gkneutomotive[.]comは悪意あるドメイン名でした。レジストラはすでにそのことを知らされているのかもしれません。というのも、以下のスクリーンショットで示す通り、このドメイン名が停止されていたためです。



*gkneutomotive[.]com*のスクリーンショット

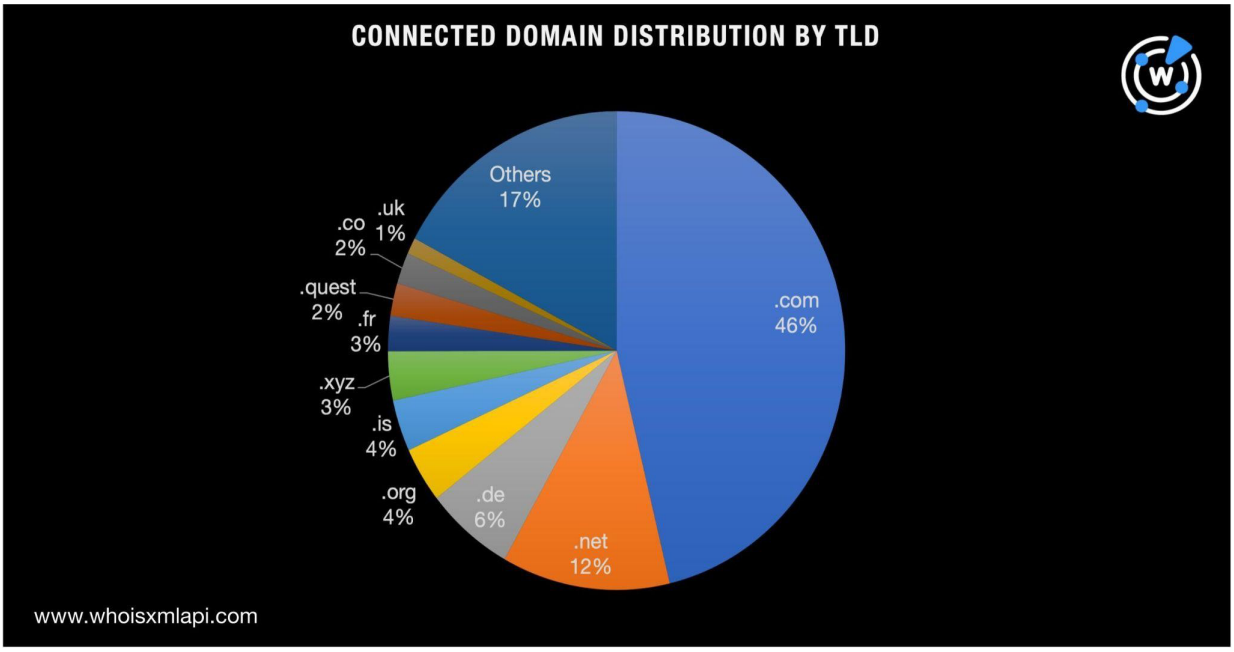
次に、上記のIPアドレス15個をbulk IP geolocation lookupで検索したところ、地理的に7カ国に散らばっていたことがわかりました。9個は米国に、その他はフランス、ドイツ、インド、インドネシア、日本およびオランダに1個ずつ位置していました。

また、13個のドメインIoCをbulk WHOIS lookupで調べた結果、1996年2月から2022年8月までの期間に登録されていたことが判明しました。また、登録者の居住国が公開されていたのはそのうち6個のみで、4個は米国、残りの2個はアイスランドで登録されていました。全てのIoCのWHOISレコードはプライバシー保護のため非公開となっていましたが、こうしたことは、正規のドメイン名ではあまり見られないことです。

13個のドメイン名のうち、WHOISデータの非公開化が増える以前に登録された最も古い2つ — click[.]org（1996年に登録）とsubmit[.]org（1998年に登録）— について、過去のWHOISレコードを検索してみました。その結果、submit[.]orgの2018年5月15日付けWHOISレコードにおいて、未編集の登録者メールアドレスを1つ発見しました。

このメールアドレスをreverse WHOIS searchにかけたところ、同じメールアドレスを使っている79個のドメイン名が新たに特定されました。そのうちの1つ、dcchosting1[.]wsは、マルウェアホストでした。本稿執筆時点で、このドメイン名は到達不能でした。

さらに、関連しているドメイン名がどのTLDを使っているかを調査しました。この作業では、サンプルとして同じIPアドレスを共用しているドメイン名を使用しました。分析の結果、.comが全サンプルの46%を占めて最も多く、次いで.net（12%）、.de（6%）、.org（4%）、.isと.xyz（各3%）、.fr、.questおよび.co（各2%）、.uk（1%）の順となりました。残りの17%は、他の108のTLDを使っていました。以下は、TLDごとのドメイン名の分布を示しています。

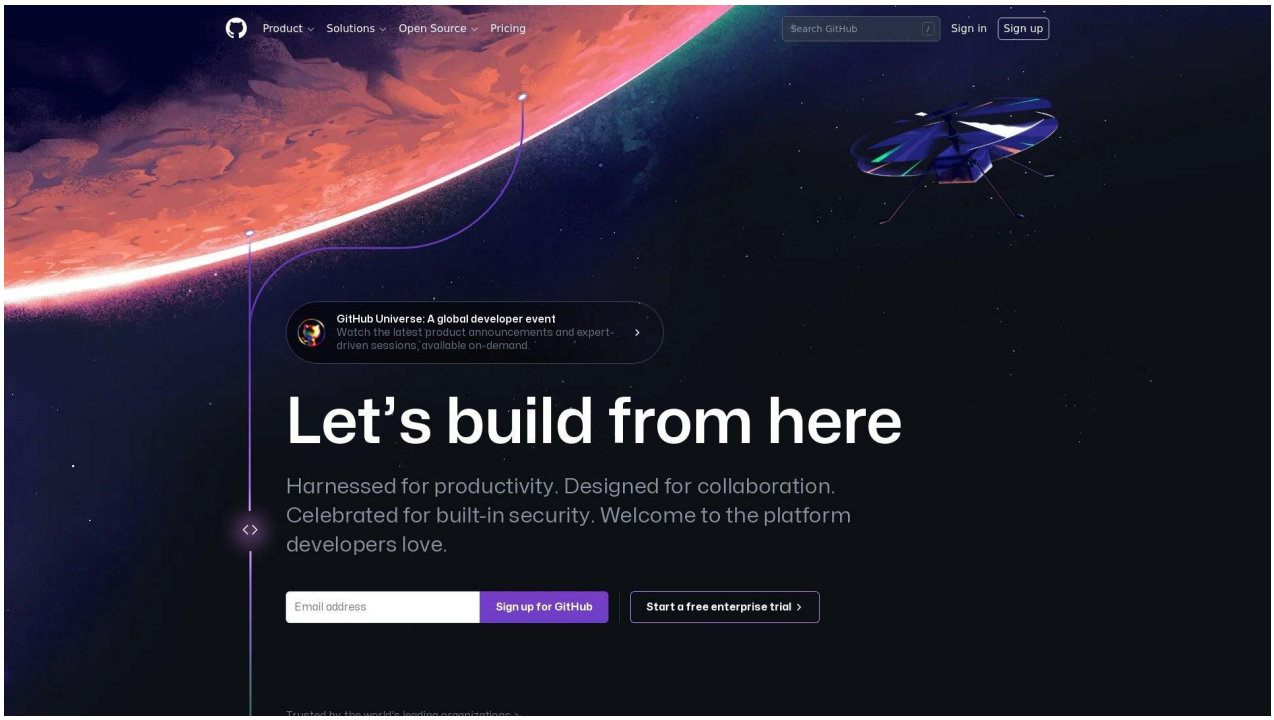


また、Nevadaの脅威アクターが以下の文字列を含んだドメイン名を使っていることに着目しました。

- ***github.***
- ***click.***
- ***continue.***
- ***repository.***
- ***signup.***
- ***submit.***

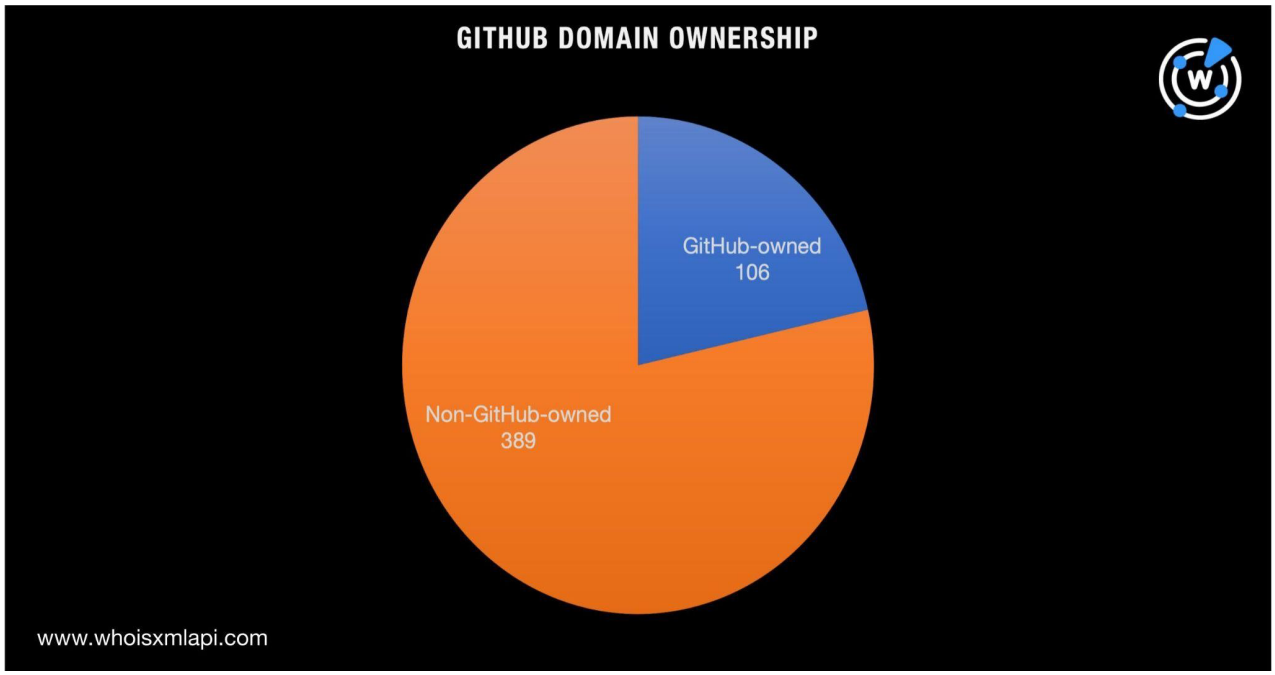
これらの文字列を含むドメイン名を当社のDomains & Subdomains Discoveryで検索したところ、2,098個の新たなドメイン名が判明しました。そのうち、click[.]hn、github[.]camおよびsignup[.]questは悪意あるドメイン名と確認されました。

なお、github[.]camはGitHubのロゴと名称を使っているにも関わらず、GitHubの正規のドメイン名であるgithub[.]comとWHOISレコードの共通点が一切ありませんでした。このことから、github[.]camはGitHubの人気を不正に利用する目的で作られたサイバースクワッティングサイトである可能性が高いと言えます。



Screenshot of github[.]cam

実際、***github***を含む495個のドメイン名のうち、WHOISのアウトプットで表示される登録者の組織名からGitHub, Inc.に帰属しているかもしれないと思われたものは、106個にとどまりました。



—

今回、既存のIoCリストの拡張分析によってDNSにおけるNevadaの足跡を辿ってみました。その結果、IoCとして今まで公表されていなかった3,000超の関連ドメイン名と7個のIPホストが追加で見つかりました。

また、この調査により、公開IoCリストに含まれていないと思われる悪意のドメイン名が5個発見されました。そして、最も悪用されているTLDを特定することもできました。こうしたインテリジェンスは、ウェブプロパティの選別を通した脅威の監視やブロックに役立てることができます。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

IoCとされたドメイン名が名前解決したIPアドレスの例

- 52[.]33[.]207[.]7
- 44[.]230[.]85[.]241
- 44[.]235[.]97[.]57
- 52[.]27[.]32[.]170

IoCの登録者メールアドレスを共用していたドメイン名の例

- geekwear[.]com
- domainwatcher[.]com
- xn--qei8618m[.]ws
- emojis[.]ws
- winslots[.]ws
- usa-merchant[.]com
- xn--qei2808m[.]ws
- get-a-name[.]com
- get-a-host[.]com
- xn--57hz0a[.]ws
- xn--qeiz728m[.]ws
- xn--xj8haa[.]ws
- worksuccess[.]ws
- wesmile[.]ws
- xn--k78h[.]ws
- dcchosting1[.]ws
- xn--fz7h[.]ws
- whassup[.]ws
- xn--5h8h[.]ws
- xn--57h9759n[.]ws

IoCのIPアドレスを共用していたドメイン名の例

- aaftech[.]me
- aasise[.]com
- abbvla[.]com
- accsetup[.]com
- adityebirla[.]com
- adnoc[.]world
- adnocbh[.]com
- adnocipo[.]org
- adnocqa[.]com
- adnocsa[.]com
- advantagepointlegal[.]com
- agdevtracker[.]org

- agfgroup[.]org
- aideepflex[.]com
- aika[.]gr
- almezmar[.]com
- almezmar[.]net
- almezmar[.]org
- alruwadalarab[.]online
- amadeuslabscampus[.]com
- amigodelosninos[.]org[.]ar
- anaviegas[.]pt
- apartment-doreen[.]rent
- apartment-rio-sky[.]com
- api[.]wadetrim[.]dev
- apieproject[.]com
- appasp[.]org[.]br
- arvaryexpress[.]store
- aspenlungconference[.]org
- atlanticglobal[.]co[.]uk
- att[.]limited
- austurborg[.]is
- aversi[.]growthhunters[.]io
- axieinifinity[.]org
- beertech[.]com
- binaural[.]fm
- bitrefill[.]io
- bjartahlid[.]is
- bjjede[.]nl
- bjkfanstoken[.]com
- blblash[.]com
- bluewatercaravanpark[.]com[.]au
- bodylanguage[.]ge
- borgarskjalasafn[.]is
- braincopy[.]ai
- brakarborg[.]is
- breadorcircus[.]com
- brekkuborg[.]is
- bsaccountancy[.]com
- btaspodcast[.]com
- bubiai[.]com
- bufferinsurancebrokers[.]com
- business146-3[.]web-hosting[.]com
- carlosvinosbaettig[.]co
- cashcard[.]ng
- ccl-chlna[.]com
- chistywelfarefoundation[.]com
- ciba-insite[.]com
- cihanyakar[.]com
- cimaplus[.]net
- ckapp[.]xyz
- click-sstech-432398472[.]us-west-2[.]elb[.]amazonaws[.]com
- clickad[.]network
- cloudbriefs[.]dev
- cobeeslliquor[.]com
- comettraining[.]org
- consultaciudadanamigraciones[.]cl
- contentexpertinc[.]com
- contentexpertinc[.]info
- contentexpertinc[.]net
- contentexpertinc[.]org
- contentreel[.]design
- costacomparte[.]cl
- criderlabs[.]com
- cuanesintranet[.]com
- cuanesthesiajobs[.]org
- cucrash[.]org
- culungspore[.]org
- cuphysicaltherapy[.]org
- curtis-dev[.]com
- customerscanvashub[.]com
- cusurgery[.]com
- cvvvt[.]co
- dailyreviewforyou[.]com
- dairycare[.]in
- damax[.]io
- dashboard[.]clickad[.]network
- datadrivends[.]com
- davlearn[.]com
- decentralized[.]gold
- defilab[.]finance

- demoversion[.]dairycare[.]in
- desert[.]cv
- destinyhealthcare[.]net
- digimatters[.]com
- digitalbus[.]kz
- digitalfranchiseguide[.]com
- digiword[.]com
- digiwrite[.]co[.]uk
- distel-gmbh[.]gq

github、*click*、*continue*、*repository*、*signup*または*submit*を含むドメイン名の例

- click[.]xn--mk1bu44c
- click[.]com[.]ng
- click[.]gen[.]tr
- click[.]management
- click[.]com[.]hn
- click[.]solar
- click[.]biz[.]pl
- click[.]tools
- click[.]enterprises
- click[.]game
- click[.]gda[.]pl
- click[.]sbs
- click[.]com[.]mt
- click[.]com[.]eg
- click[.]moscow
- continue[.]reviews
- continue[.]rentals
- continue[.]cruises
- continue[.]institute
- continue[.]gratis
- continue[.]pub
- continue[.]lol
- continue[.]me
- continue[.]care
- continue[.]run
- continue[.]video
- continue[.]sk
- continue[.]cloud
- continue[.]ai
- continue[.]cz
- github[.]okinawa
- xn--thub-kxa4d[.]ws
- github[.]sexy
- github[.]recipes
- github[.]io2222
- xn--githu-hkc[.]ws
- github[.]market
- github[.]tw
- github[.]host
- github[.]la
- github[.]tel
- github[.]luxe
- github[.]software
- github[.]rip
- github[.]family
- repository[.]in
- repository[.]group
- repository[.]gdn
- repository[.]edu[.]sd
- repository[.]ai
- repository[.]host
- repository[.]biz[.]id
- repository[.]co[.]il
- repository[.]io
- repository[.]id
- repository[.]it
- repository[.]xyz
- repository[.]healthcare
- repository[.]cfd
- repository[.]photos
- signup[.]men
- signup[.]foundation

- signup[.]website
- signup[.]no
- signup[.]dk
- signup[.]im
- signup[.]jobs
- signup[.]army
- signup[.]menu
- signup[.]fun
- signup[.]dance
- signup[.]co[.]in
- signup[.]aws
- signup[.]casa
- signup[.]best
- submit[.]flowers
- submit[.]xin
- submit[.]tk
- submit[.]jp
- submit[.]pub
- submit[.]social
- submit[.]faith
- submit[.]yachts
- submit[.]es
- submit[.]sk
- submit[.]expert
- submit[.]ws
- submit[.]kr
- submit[.]website
- submit[.]agency
- submit[.]host
- submit[.]report
- submit[.]gg
- submit[.]money
- submit[.]rocks
- submit[.]rent
- submit[.]memorial
- submit[.]nyc
- submit[.]by
- submit[.]cl