Searching for Nevada Ransomware Digital Crumbs in the DNS

Table of Contents

Executive Report

Resecurity threat researchers discovered a new ransomware they've dubbed "Nevada" being sold on the RAMP underground community. Their analysis of the malware showed it underwent several upgrades in January 2023 alone. Primarily distributed to non-English-speaking threat actors via the ransomware-as-a-service (RaaS) model in the Dark Web, Nevada ransomware has been plaguing both Windows and Linux computer users.

Using a list of indicators of compromise (IoCs) comprising seven IP addresses and 13 domains from AlienVault OTX, WhoisXML API searched for Nevada ransomware digital crumbs in the DNS. The following table shows the original IoC list.

IP ADDRESSES	DOMAINS
• 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

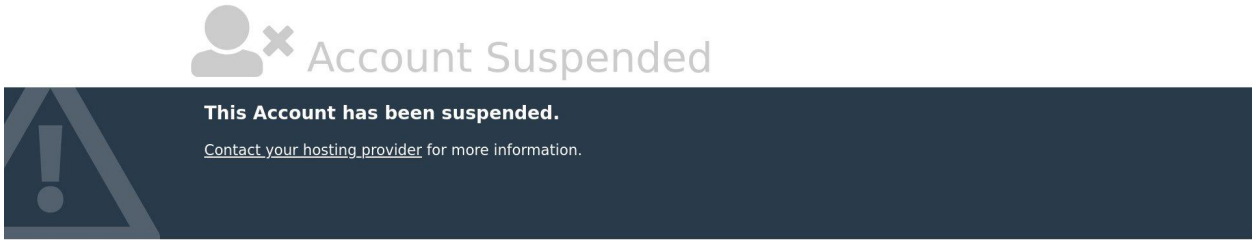
Our deep dive led to the discovery of:

- Eight additional IP addresses to which the domains identified as IoCs resolved
- One unredacted registrant email address from the historical WHOIS records of one of the domain IoCs
- 79 additional domains that shared one of the IoCs' registrant email address, one of which turned out to be malicious
- 1,178 additional domains that shared some of the IoCs' IP hosts, one of which turned out to be a malware host
- 2,098 additional domains that contained the strings ***github.***, ***click.***, ***continue.***, ***repository.***, ***signup.***, and ***submit.***, three of which turned out to be malicious

Nevada Ransomware Digital Crumb Revelations

DNS lookups for the 13 domain IoCs allowed us to uncover eight IP addresses that aren't part of the original IoC list. Reverse IP lookups for these additional IP addresses and the seven that have already been identified as IoCs revealed that four of them were dedicated hosts, another four were shared hosts, and seven didn't have IP resolutions.

The reverse IP lookups also provided a list of 1,178 more domains. Of these, only one—gkneutomotive[.]com—turned out to be malicious. Its registrar may have already been made aware of its nature since its owner's registration has been suspended as evidenced by the screenshot below.



Screenshot of gkneutomotive[.]com

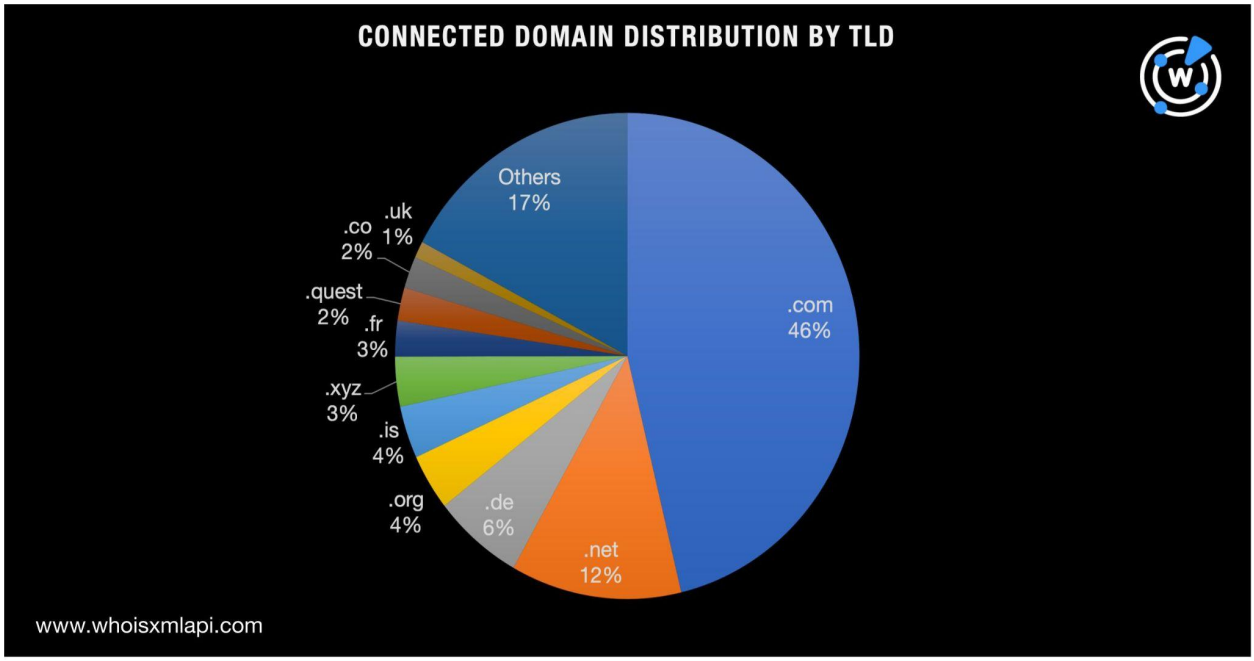
Next, a bulk IP geolocation lookup for the 15 IP addresses revealed they were scattered across seven countries. Nine of the IP addresses were geolocated in the U.S. while one each pointed to France, Germany, India, Indonesia, Japan, and the Netherlands.

Subjecting the 13 domain IoCs to a bulk WHOIS lookup, meanwhile, showed they were created between February 1996 and August 2022. Only six of them had publicly visible registrant countries. Four of the domains were registered in the U.S. while the remaining two in Iceland. All of the IoCs' WHOIS records were also privacy-protected or have been redacted, which isn't typical of legitimate domains.

A closer look at the historical WHOIS records of the two oldest domains created before WHOIS redaction became widespread, click[.]org (created in 1996) and submit[.]org (created in 1998), led to the discovery of an unredacted registrant email address for the latter's WHOIS record dated 15 May 2018.

A reverse WHOIS search for this registrant email address gave us 79 additional domains. One of them—dcchosting1[.]ws—turned out to be a malware host. It is unreachable as of this writing.

To ease domain monitoring for security teams, we sought to identify the TLD extensions the connected domains used. For that, we utilized the IP-connected domains as our sample. Our analysis revealed that .com led the pack, accounting for 46% of the total domain volume, followed by .net (12%); .de (6%); .org (4%); .is and .xyz (3% each); .fr, .quest, and .co (2% each); and .uk (1%). The remaining 17% was spread across 108 other TLDs. Take a look at the domain distribution by TLD chart below.

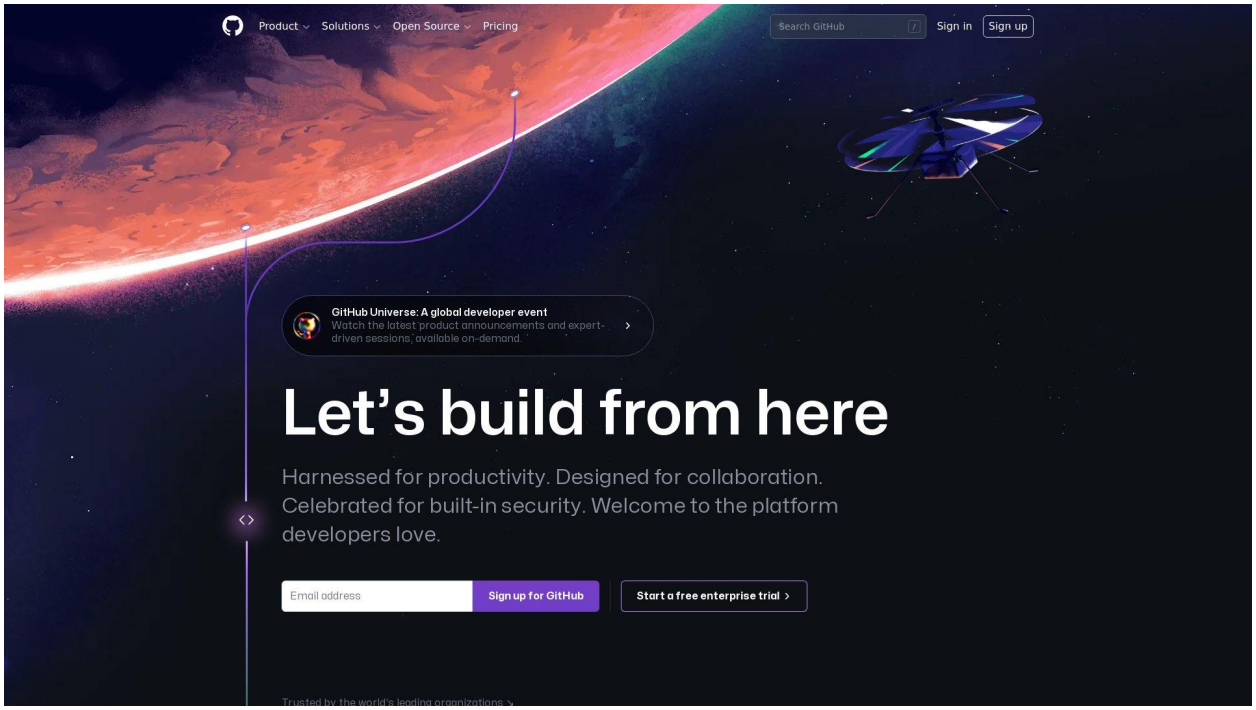


We also noticed the Nevada ransomware threat actors' use of the following strings in their domains:

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

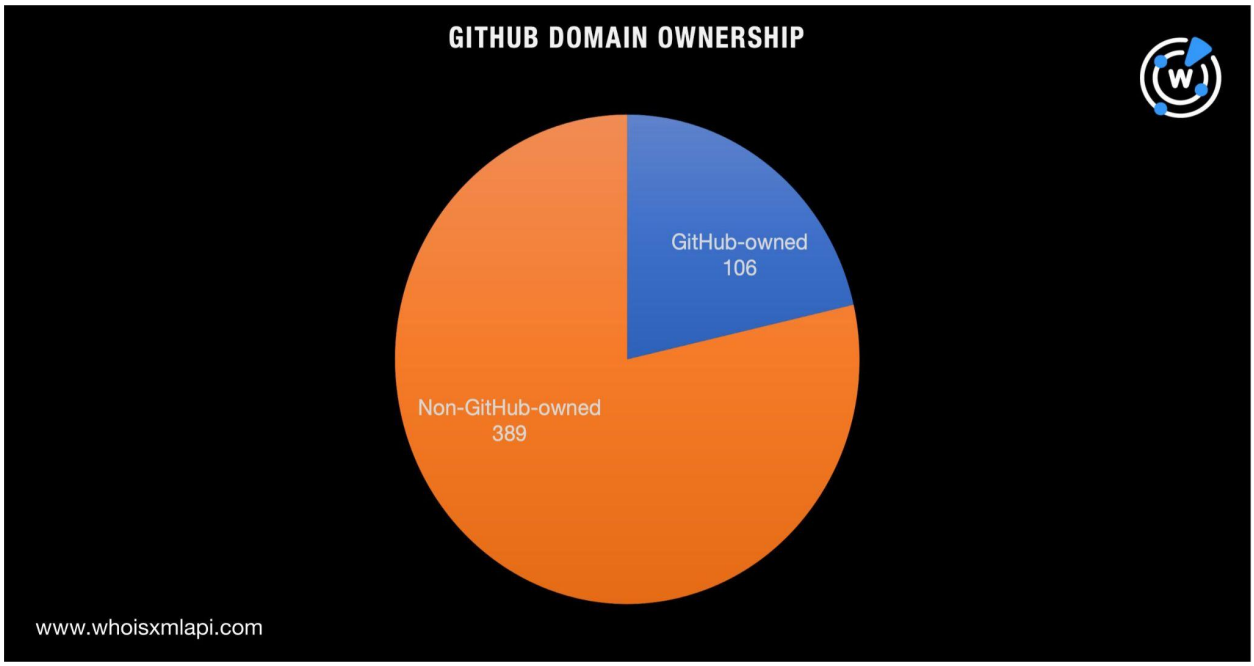
Our Domains & Subdomains Discovery searches for domains containing these strings uncovered 2,098 additional domains, three of which turned out to be malicious. These dangerous web properties were click[.]hn, github[.]cam, and signup[.]quest.

Note that despite github[.]cam's usage of the GitHub logo and name, it doesn't share any WHOIS record commonalities with the legitimate domain github[.]com. As such, it's more likely to be a cybersquatting site designed to take advantage of GitHub's popularity.



Screenshot of github[.]cam

In fact, among the 495 ***.github***-containing domains, only 106 could be publicly attributed to GitHub based on their registrant organization, GitHub,Inc.



—

Our search for Nevada ransomware digital crumbs in the DNS through an IoC expansion analysis uncovered more than 3,000 possibly connected domains and seven IP hosts that haven't been publicized as IoCs.

This study also led to the discovery of five malicious domains that may not be part of any publicly accessible IoC list to date. We were also able to identify the most-abused TLDs that could aid in prioritizing web properties for threat monitoring and consequent blocking.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

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

Sample Domains That Shared an IoC's Registrant Email Address

- 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

Sample Domains That Shared the IoCs' IP Hosts

- 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

Sample Domains That Contained the Strings *github.*, *click.*, *continue.*, *repository.*, *signup.*, or *submit.*

- 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