Is Aurora as Stealthy as Its Operators Believe?

Table of Contents

Executive Report

Stealth is a typical goal for most threat actors when launching malware and other attacks. The better hidden a malware is, the more effective an attack becomes. And that is what fast-rising data stealer Aurora is gaining notoriety for.

Former bot maker-turned-data stealer Aurora's rise to stardom has, in fact, recently piqued SEKOIA.IO researchers' interest, leading them to publish 51 indicators of compromise (IoCs)—including 28 IP addresses and eight domains—related to the threat. Is Aurora truly flying under the radar, though? Or can extensive WHOIS, IP, and DNS intelligence point to more digital breadcrumbs?

Our IoC expansion exercise, which jumped off the IoCs SEKOIA.IO researchers already identified, led to the discovery of:

- One unredacted email address used to register one of the domains identified as IoCs
- Four additional IP addresses to which some of the IoCs resolved
- 972 more domains that resolved to some of the IoCs' IP hosts, 43 of which turned out to be malicious
- 2,262 additional domains that shared unique strings found among the IoCs, seven of which were categorized as malware hosts

IoC Expansion Revelations

WHOIS Connections

We began our deep dive into Aurora with a bulk WHOIS lookup for the domains identified as IoCs. Three of them—onesoftware[.]site, unisoft[.]store, and mividajugosa[.]com—had retrievable WHOIS records. While onesoftware[.]site and unisoft[.]store didn't have registrant email addresses on file, mividajugosa[.]com did.

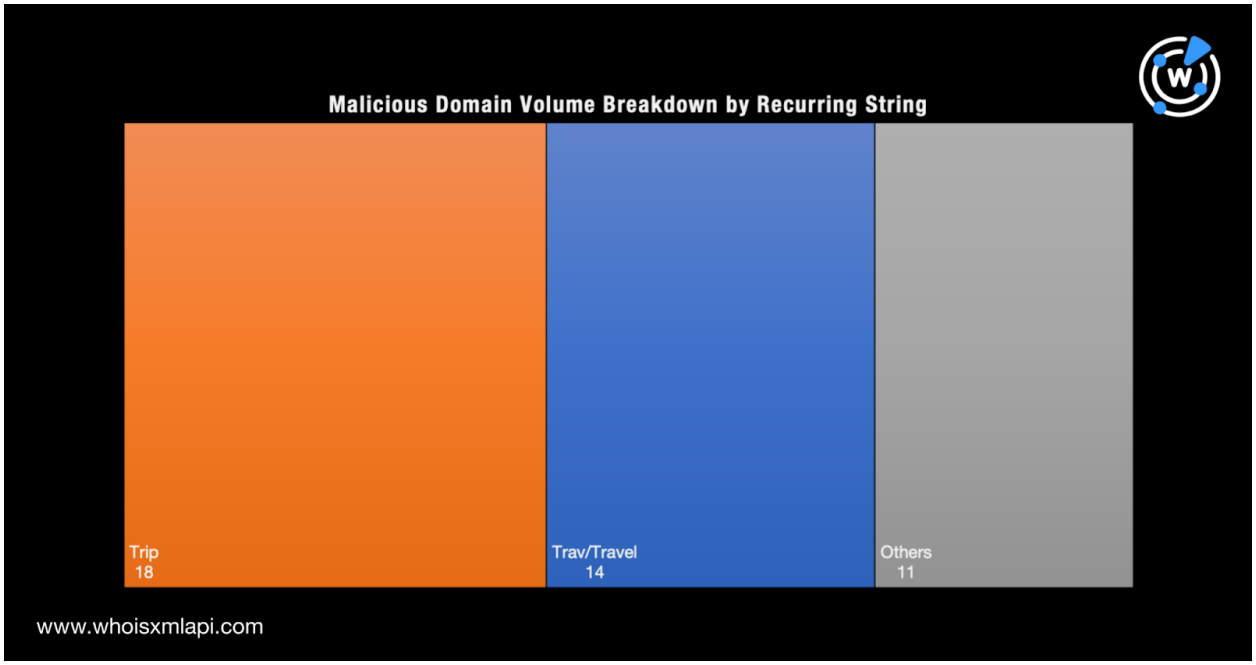
A historical reverse WHOIS search for mividajugosa[.]com's unredacted registrant email address showed it has only been used to register the corresponding IoC. Could the registrant be affiliated with the threat group behind Aurora? Did she abandon the domain when it was flagged as malicious?

DNS Connections

Next, DNS lookups for the eight domains identified as IoCs allowed us to uncover an additional four IP addresses (e.g., 79[.]137[.]197[.]201 and 91[.]229[.]90[.]149) that aren't on the publicized list. While none of them are considered malicious to date, they all manifested Secure Sockets Layer (SSL) configuration issues that could make them prone to compromise.

Further scrutiny via reverse IP lookups for the IP addresses identified as IoCs and the four others we uncovered led to the discovery of 972 domains that could be connected to the threat. In fact, 43 of these domains turned out to be malicious after a bulk malware check.

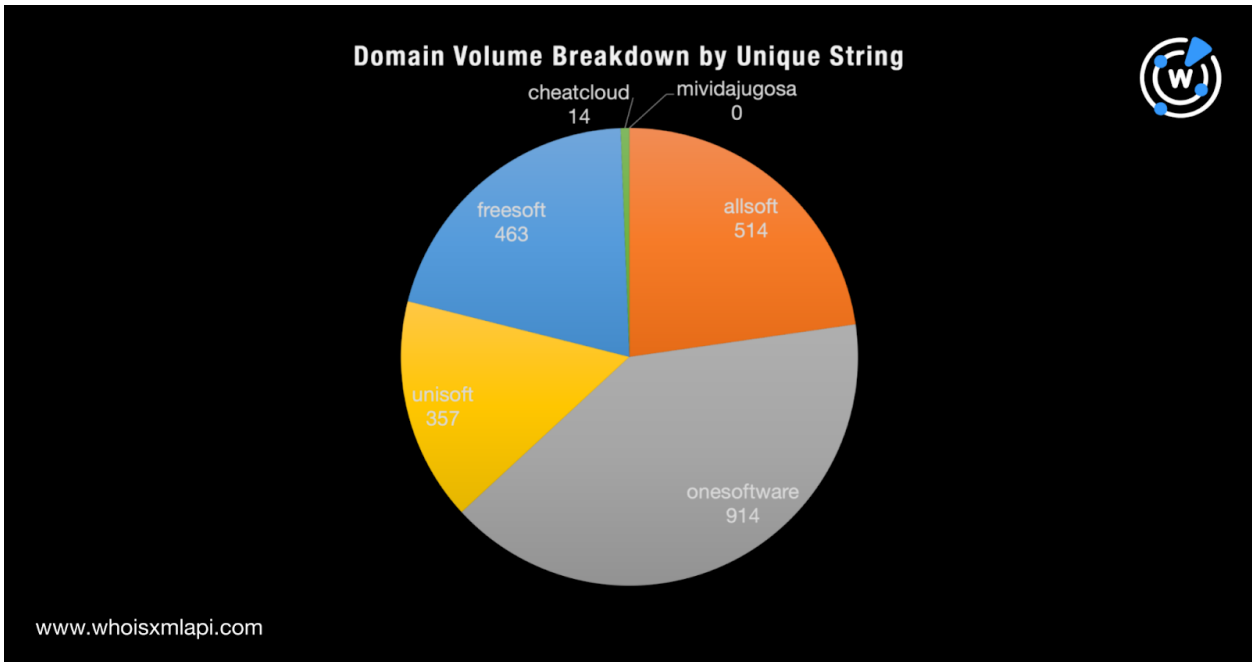
A closer look at the malicious domains showed that a majority could be travel-themed, given the appearance of strings like "trav," "travel," and "trip." Here's a domain volume breakdown for the strings.



More “trip”-containing domains were found compared with those with the string “trav” or “travel.”

Domain String Connections

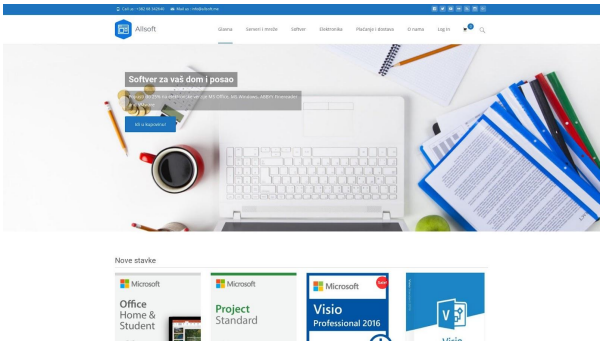
We noticed unique strings among the domains identified as IoCs, namely, “allsoft,” “onesoftware,” “unisoft,” “freesoft,” “cheatcloud,” and “mividajugosa.” Using these as Domains & Subdomains Discovery search terms allowed us to uncover 2,262 additional domains, seven of which turned out to be malware hosts. Examples of the malicious web properties are cheatcloud[.]us, cheatcloud[.]fun, cheatcloud[.]pro, and cheatcloud[.]one. Here’s a breakdown of the additional domains we found by unique string.



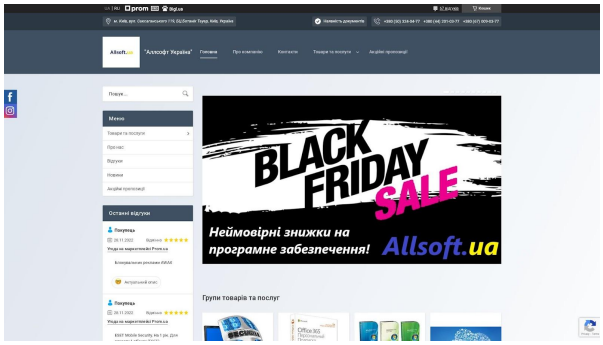
“Soft” appeared in 99% of the domains, potentially alluding that visitors can obtain free copies of the programs featured on the websites they hosted.

Screenshot Connections

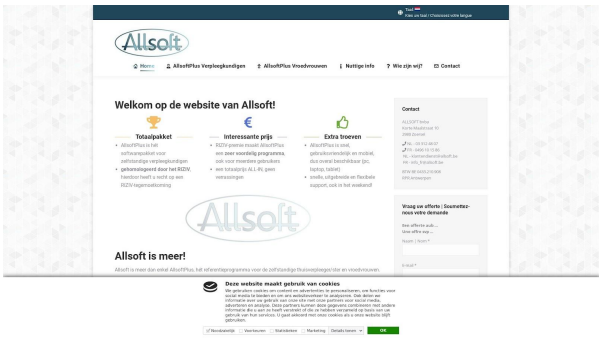
Screenshot lookups for the 2,262 additional domains we can consider potential threat artifacts also yielded an interesting result. We found that “allsoft” is commonly used by several websites offering application downloads or software development services. The actors behind Aurora may be mimicking these seemingly legitimate country-specific sites to lure users to click their malicious links.



Screenshot of allsoft[.]me



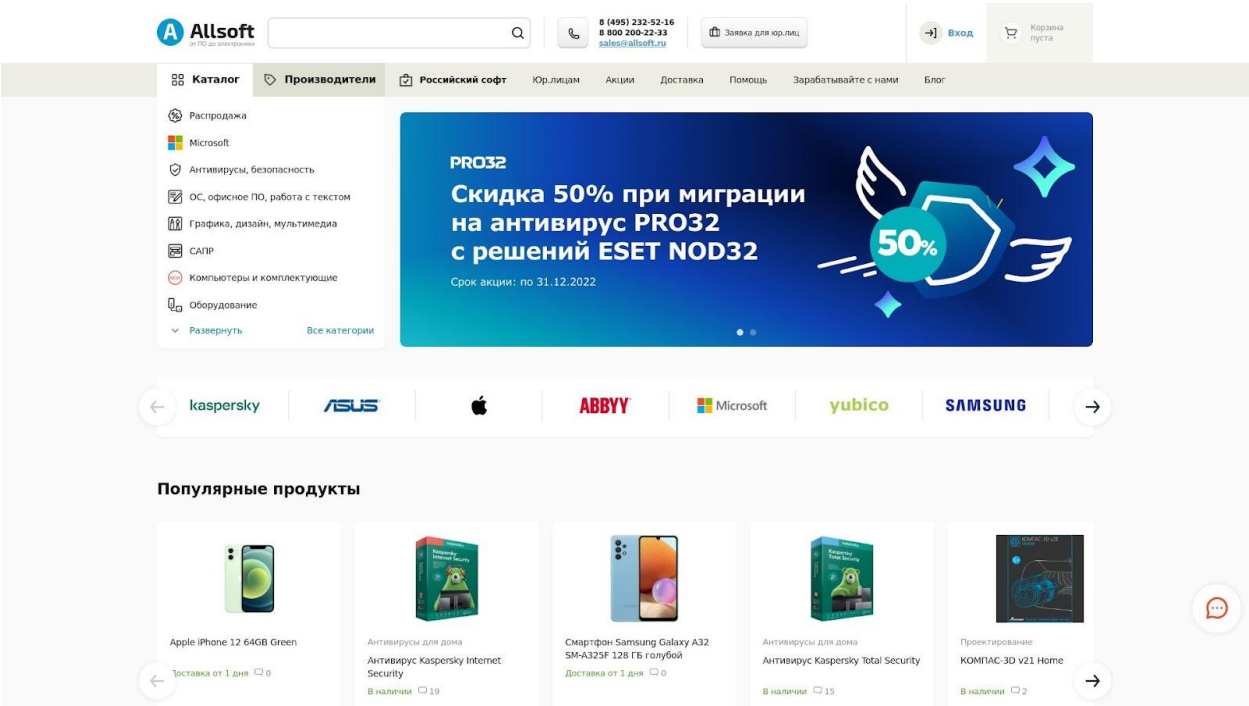
Screenshot of allsoft[.]ua



Screenshot of allsoft[.]be

Given the country-code top-level domains (ccTLDs) used, users from Montenegro (.me), Ukraine (ua), and Belgium (.be) interested in downloading applications from the three sites above should be wary of clicking the IoCs allsofts[.]cloud and alls0ft[.]cloud.

In addition, at least eight of the “allsoft” sites hosted the same content, which could mean they’re localized versions of two companies’ business pages.

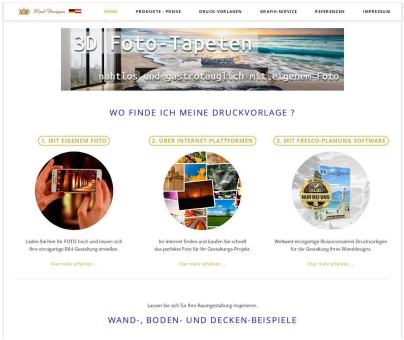


Screenshot of allsoft[.]uz, allsoft[.]su, allsoft[.]by, allsoft[.]kz, and allsoft[.]ru

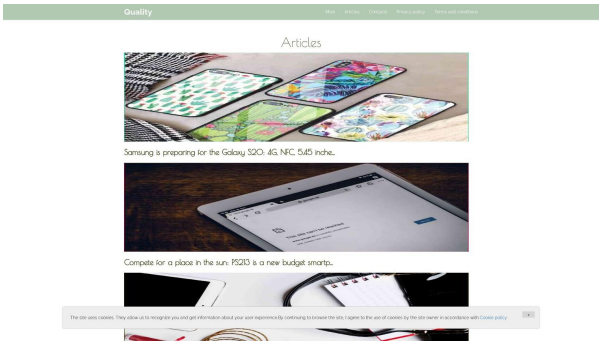
Screenshot of allsoft[.]co, allsoft[.]us, and allsoft[.]in

Customers of the software download site and the software development company should also steer clear of the “allsoft” IoCs SEKOIA.IO identified.

One “allsoft” domain oddly hosted what looked to be a 3D photo development site. Interestingly, the domain appeared similar to the IoC alls0ft[.]cloud that pointed to what looked like a blog about the latest tech gadgets.



Screenshot of the artifact allsoft[.]at



Screenshot of the IoC alls0ft[.]cloud

—

Our IoC expansion effort led to the identification of 3,188 potentially connected artifacts and possibly 50 additional IoCs that likely require blocking for utmost protection. Returning to the question of whether Aurora is truly flying under the radar, the digital breadcrumbs we uncovered may lead to further transparency on the threat group’s activities.

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

IoCs SEKOIA.IO Identified

IP Addresses	Domains
• 138[.]201[.]92[.]44 • 146[.]19[.]24[.]118 • 167[.]235[.]233[.]95	• winsofts[.]cloud • allsofts[.]cloud • alls0ft[.]cloud

• 185[.]173[.]36[.]94 • 185[.]209[.]22[.]98 • 193[.]233[.]48[.]15 • 37[.]220[.]87[.]2 • 45[.]137[.]65[.]190 • 45[.]144[.]30[.]146 • 45[.]15[.]156[.]115 • 45[.]15[.]156[.]22 • 45[.]15[.]156[.]33 • 45[.]15[.]156[.]80 • 45[.]15[.]156[.]97 • 45[.]15[.]157[.]137 • 49[.]12[.]222[.]119 • 49[.]12[.]97[.]28 • 5[.]9[.]85[.]111 • 65[.]108[.]253[.]85 • 65[.]109[.]25[.]109 • 78[.]153[.]144[.]31 • 79[.]137[.]195[.]171 • 81[.]19[.]140[.]21 • 82[.]115[.]223[.]218 • 85[.]192[.]63[.]114 • 89[.]208[.]104[.]160 • 95[.]214[.]55[.]225	• onesoftware[.]site • unisoft[.]store • freesoft[.]digital • cheatcloud[.]info • mividajugosa[.]com

Sample Domains That Shared the IoCs' IP Hosts

- 1188[.]fit
- 1callfix[.]in
- 1kplus[.]info
- 2x2y[.]online
- 30contyno[.]space
- 3rdgroup[.]consulting
- aaron-cortez[.]net
- abdullahfarmhouses[.]com
- abdulrahmanonline[.]space
- abidacottrell[.]website
- academy[.]designhub247[.]com
- acarcelikunltd[.]com
- accountantswithoutborders[.]johnsonbookkeeping[.]online
- accountantswithoutborders[.]org
- additionfe[.]click
- adecreates[.]com
- adguru[.]ga
- adsofbd[.]com
- afterburner[.]site
- afterburner[.]space
- afterburner[.]website
- agencasino[.]org
- agrocap[.]com[.]do
- agrokorna[.]com
- agropoint[.]az
- aiaedificaciones[.]com[.]mx
- aimengqiu[.]tk

- aimengqiu01[.]tk
- aiowoman[.]com[.]ng
- airfryer4u[.]com
- airtimeswap[.]com
- akonlyak[.]mooo[.]com
- akonlyak[.]online
- akonlyak[.]ru
- al-hijin[.]co
- albertawebsolutions[.]com
- albrighton-group[.]co[.]uk
- aldoushuxleymortonstudio[.]site
- alejandromolinamd[.]com
- alghandour[.]net
- alhaq[.]in
- alhaya-medical[.]com
- alhaya-medical[.]riyadhpharma[.]com
- alice-business[.]tk
- alicelindsey[.]space
- alicelindseylive[.]space
- aliurdunews[.]com
- allalicelindsey24[.]space
- allannaliesegroup[.]website
- allannaliesellc[.]website
- allblackssouthafrica[.]com
- allblacksvsire[.]com
- allblacksvswalla[.]com
- allcourtneyjadencarlson[.]space
- alldottycooperdesign[.]nguyenbinhcomputer[.]com
- alldottycooperdesign[.]space
- allemmettmoreno[.]site
- allenreding[.]com
- allfelixgirlvan[.]site
- allgracie[.]space
- alllblacksvsargentina[.]com
- alllblacksvswalla[.]com
- allmacsenestrada[.]site
- allmahcutonline[.]website
- allndolan[.]site
- allnwatkinsnow[.]space
- alls0ft[.]cloud
- alls0ftware[.]cloud
- allshaniatoddshop[.]space
- allsoft[.]cloud
- allsofts[.]cloud
- allsoftware[.]cloud
- allsoftware[.]space
- alltaibaemery[.]site
- alltmoreno[.]website
- allwritingpro[.]com
- allzoenight[.]website
- alotaxitrebinje[.]com
- alumco[.]mx
- alwynvelasquezusa[.]site
- amberre[.]click
- ameliaclub[.]space
- ameliasolutions[.]space
- ammarhu[.]site
- ammarhublog[.]site
- ammlp[.]click
- amras[.]in
- anabelleparrish[.]site
- analytictree[.]com
- anarmahindrarish[.]site
- anarmentorishdesign[.]site
- anarrish[.]site
- anatoliamuzikdans[.]anatoliasanatmerkezi[.]com[.]tr
- anatoliasanatmerkezi[.]com[.]tr
- andmahaveerpenni[.]site
- androscrabfarm[.]com
- andveerpenni[.]site
- anegod[.]tk
- anfei[.]tk
- angrewei[.]cf

Sample Malicious Domains That Shared the IoCs' IP Hosts

- bastrips[.]online
- bastrips[.]ru
- bestrips[.]ru
- brooktravel[.]online
- carteena[.]ml
- cheatcloud[.]us
- gustrips[.]ru
- hustravel[.]online
- hustravel[.]ru
- hustrips[.]online
- investment[.]j-dee[.]ml
- j-dee[.]ml
- launmansnw[.]co
- mail[.]bestrips[.]ru
- mail[.]carteena[.]ml
- mail[.]gustrips[.]ru
- mail[.]pastrip[.]ru
- mail[.]pastrips[.]online
- mail[.]rastrips[.]online
- mail[.]s472911[.]ha003[.]t[.]justns[.]ru

Sample Domains That Shared the IoCs' Unique Strings

- allsoft[.]uz
- allsoft[.]cf
- allsoft[.]hu
- allsoft[.]nu
- allsoft[.]mn
- allsoft[.]se
- allsoft[.]cz
- allsoft[.]ua
- allsoft[.]ch
- allsoft[.]ro
- allsoft[.]de
- allsoft[.]be
- allsoft[.]it
- allsoft[.]vn
- allsoft[.]uk
- allsoft[.]ao
- allsoft[.]io
- allsoft[.]mx
- allsoft[.]ir
- allsoft[.]tj
- allsoft[.]co
- allsoft[.]su
- allsoft[.]nl
- allsoft[.]ee
- allsoft[.]cl
- allsoft[.]at
- allsoft[.]by
- allsoft[.]tk
- allsoft[.]eu
- allsoft[.]us
- allsoft[.]cc
- allsoft[.]me
- allsoft[.]kz
- allsoft[.]ru
- allsoft[.]fr
- allsoft[.]gr
- allsoft[.]cn
- allsoft[.]ga
- allsoft[.]pl
- allsoft[.]in
- allsoft[.]no
- allsoft[.]biz
- allsoft[.]pro
- hallsoft[.]nl
- vallsoft[.]tk
- allsoft[.]icu

- ballsoft[.]de
- allsoft[.]com
- aallsoft[.]tk
- onesoftware[.]co
- onesoftware[.]su
- onesoftware[.]ru
- onesoftware[.]my
- onesoftware[.]eu
- onesoftware[.]no
- onesoftware[.]cl
- onesoftware[.]fr
- onesoftware[.]nl
- onesoftware[.]it
- onesoftware[.]uk
- onesoftware[.]cz
- onesoftware[.]io
- onesoftware[.]ro
- onesoftware[.]us
- onesoftware[.]se
- onesoftware[.]gq
- zonesoftware[.]tk
- onesoftware[.]xyz
- onesoftware[.]pro
- unisoft[.]az
- unisoft[.]kz
- unisoft[.]dk
- unisoft[.]by
- unisoft[.]ru
- unisoft[.]cz
- unisoft[.]am
- unisoft[.]ua
- unisoft[.]no
- unisoft[.]id
- unisoft[.]lk
- unisoft[.]mx
- unisoft[.]ws
- unisoft[.]gr
- unisoft[.]gq
- unisoft[.]tw
- unisoft[.]uz
- unisoft[.]de
- unisoft[.]hr
- unisoft[.]ie
- unisoft[.]tk
- unisoft[.]ga
- unisoft[.]us
- unisoft[.]at
- unisoft[.]ca
- unisoft[.]jp
- unisoft[.]nl
- unisoft[.]fr
- unisoft[.]hu
- unisoft[.]ml