WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Cloud Atlas May Hide Their Tracks but 1,800+ Unpublicized Artifacts Can Help Orgs Tag Them

Table of Contents

Executive Report

Cyber espionage group Cloud Atlas has been trailing its sights on critical infrastructure operators in countries suffering from political conflict since its discovery in 2014. Aptly nicknamed “Inception,” the group’s tactic of going after nations with bigger problems than cybersecurity seems to be working, as evidenced by successful intrusions over the years.

Check Point Research (CPR) publicized the following indicators of compromise (IoCs), specifically eight domains and two IP addresses, to aid potential targets to avoid succumbing to data breaches. These IoCs are:

- translate-news[.]net
- technology-requests[.]net
- remote-convert[.]com
- protocol-list[.]com
- gettemplate[.]org
- driversolution[.]net
- desktoppreview[.]com
- comparelicense[.]com
- 185[.]227[.]82[.]21
- 146[.]70[.]88[.]123

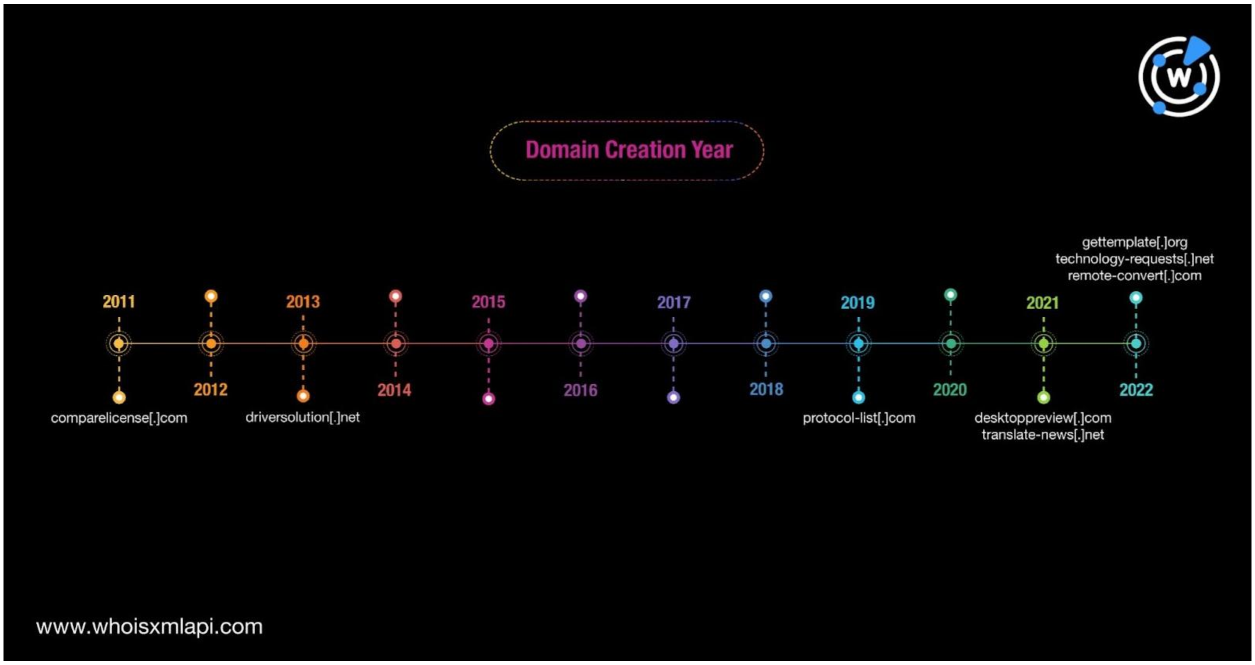
WhoisXML API researchers found more artifacts that could help with that, including:

- Eight additional IP addresses the domains identified as IoCs resolved to
- 324 additional domains that shared the IoCs’ IP hosts, two of which are malicious
- 1,519 more domains that contained unique strings found among the domains identified as IoCs, one of which is malicious

IoC Analysis Findings

Our closer look into the IoCs began with a bulk WHOIS lookup that revealed the following:

- Two of the domains tagged as IoCs—gettemplate[.]org and comparelicense[.]com—didn't have retrievable WHOIS records.
- Four of the domain IoCs were managed by two registrars—protocol-list[.]com and technology-requests[.]net indicated NetEarth One, Inc. as their registrar while driversolution[.]net and remote-convert[.]com shared PDR Ltd. d/b/a PublicDomainRegistry.com. The remaining two indicated Danesco Trading Ltd. and Internet Domain Service BS Corp. as their registrars.
- All of the domain IoCs' WHOIS records have been redacted.
- A majority of the domain IoCs were created just this year. The time line below shows their volume distribution by creation year.



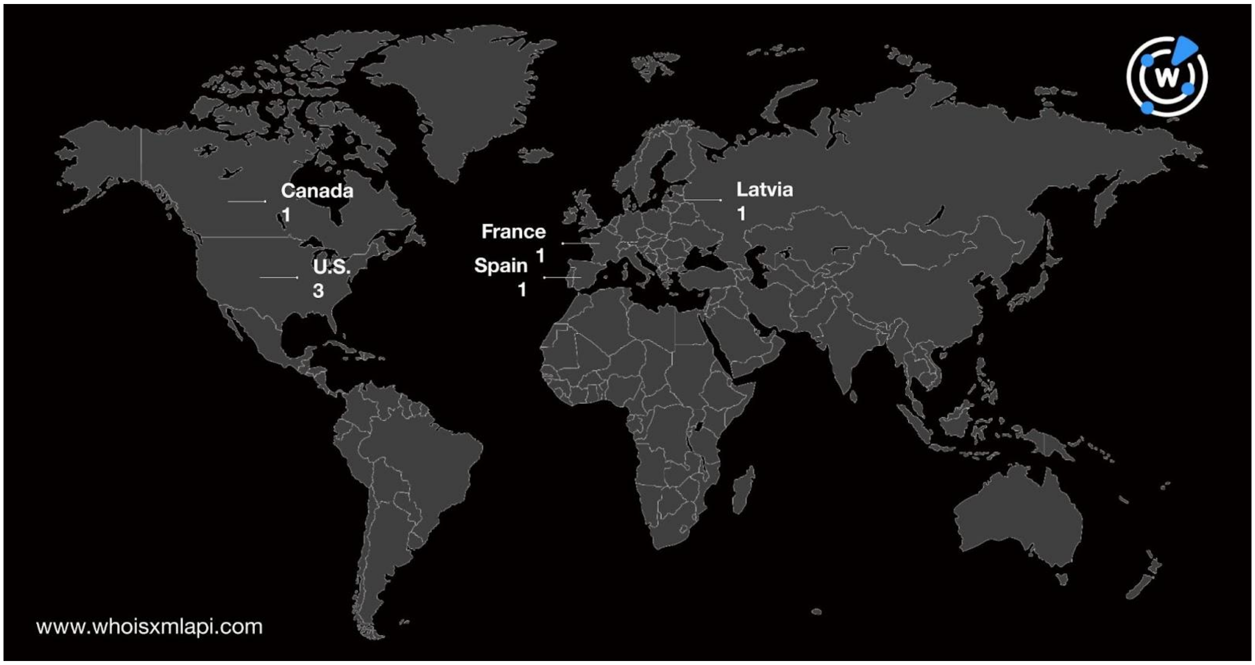
- The domain IoCs were spread across five registrant countries—the Netherlands, Finland, Cyprus, the U.K., and Canada.
- None of the domain IoCs are currently considered malicious but given their ties to Cloud Atlas, organizations may do well to block all access to them.

IP geolocation lookups for the IP addresses identified as IoCs, on the other hand, showed they didn't share any similarity. 185[.]227[.]82[.]21 was geolocated in the Netherlands with Access2.IT Group B.V. as ISP while 146[.]70[.]88[.]123 was located in France under M247 Europe SRL. Both are also considered nonmalicious but their connection to Cloud Atlas probably merits strict monitoring at the very least for signs of suspicious activity.

Given Cloud Atlas's success so far in infiltrating target networks and that it trails its sights on critical infrastructure operators, we sought to expand the current list of IoCs to enable potential future targets to mitigate the threat.

IoC Expansion Analysis

To obtain as many possibly connected artifacts as possible, we first subjected the domain IoCs to DNS lookups that led to the discovery of eight IP addresses. The bulk IP geolocation lookup revealed that 5[.]135[.]199[.]19 shared the same origin country—France—as the IoC 146[.]70[.]88[.]123. The rest were scattered across four other countries as the map below shows.



While none of the artifacts are detected as malicious, a closer scrutiny of the IP addresses revealed they all had Secure Sockets Layer (SSL) misconfigurations.

Next, reverse IP lookups for the two IP address IoCs and seven additional artifacts provided a list of 324 domains. Of these, two were found malicious—lucid-banzai[.]104-219-233-120[.]plesk[.]page and www[.]lucid-banzai[.]104-219-233-120[.]plesk[.]page.

We also noticed unique strings among the domain IoCs and used these to look for more potential connections via Domains & Subdomains Discovery:

- "translate + news"
- "technology + request"

- “remote + convert”
- “protocol + list”
- “get + template”
- “driver + solution”
- “desktop + preview”
- “compare + license”

Our inquiry uncovered 1,519 additional domains that can be considered artifacts. Fortunately, for now, only one—solutionefordriversandrestornow[.]online—is considered malicious by malware engines we queried. Examples of artifacts that resembled the IoCs most—they just used different top-level domain (TLD) extensions—include:

- translate-news[.]com
- gettemplate[.]ir
- gettemplate[.]co
- gettemplate[.]us
- gettemplate[.]de
- gettemplate[.]io
- gettemplate[.]tk
- gettemplate[.]ru
- gettemplates[.]co
- gettemplate[.]net
- gettemplate[.]com
- driversolution[.]pl
- driversolution[.]com
- driversolution[.]info
- desktoppreview[.]ws

—

The IoC expansion analysis uncovered 1,850 additional Cloud Atlas artifacts, including three malicious domains, that could put potential targets and other organizations at risk should they land on the sites these web properties hosted. Without the help of IP, DNS, and WHOIS intelligence, we wouldn’t have been able to find these connections.

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

Cloud Atlas IoCs Identified by CPR

- translate-news[.]net
- technology-requests[.]net
- remote-convert[.]com
- protocol-list[.]com
- gettemplate[.]org
- driversolution[.]net
- desktoppreview[.]com
- comparelicense[.]com
- 185[.]227[.]82[.]21
- 146[.]70[.]88[.]123

Sample IP Addresses the Domains Identified as IoCs Resolved To

- 192[.]144[.]39[.]67
- 149[.]56[.]175[.]181

- 172[.]105[.]103[.]207
- 5[.]135[.]199[.]19

Sample Domains That Shared the IoCs’ IP Hosts

- 064625[.]parkingcrew[.]net
- 0x21[.]in
- 104-219-233-120[.]plesk[.]page
- 23012002[.]com
- 2mblk[.]com
- 43nutrientes[.]com
- 548260[.]parkingcrew[.]net
- 5pneuovxi22i4fagh9[.]today
- 7-eleven-handbags[.]com
- 825610[.]parkingcrew[.]net
- 8tril[.]com
- 944279[.]parkingcrew[.]net
- a-plague-tale[.]top
- a2c491023580[.]com
- a2e6b661ca0e4c4c4[.]awsglobalaccelerator[.]com
- a5c6a0cc95db01a9[.]com
- abrakadabras[.]net
- abvtqhwodwjmi[.]work
- accemfsqovkd[.]pw
- account[.]adfs[.]kyivstar[.]online
- acerthk3v9fvsby5n[.]today
- acjhwpdjhlhbncf[.]click
- adams679[.]drcopps[.]com
- adfs[.]kyivstar[.]online
- admiral-juegos[.]com
- adobe-update[.]net
- adobestats[.]com
- adsdsadsalifsa[.]digital
- agceram[.]com
- agusanplantation[.]com
- ahsqbeospcdrngfv[.]info
- aliensdrop[.]com
- allen1037[.]pelangiqq99[.]com
- allen139[.]drcopps[.]com
- allen618[.]drcopps[.]com
- allsofttech[.]com
- amakeperfeita[.]online
- ampjsppmftmfdblpt[.]info
- anderson360[.]pelangiqq99[.]com
- anderson576[.]pelangiqq99[.]com
- anderson856[.]drcopps[.]com
- anderson858[.]drcopps[.]com
- antichltabompadre[.]com
- asdakasma[.]digital
- asiaworldremit[.]com
- assumethepositionstudio[.]com
- autoconfig[.]celikklczet[.]com
- autoconfig[.]simsekaluminyurn[.]com
- autodiscover[.]celikklczet[.]com
- autodiscover[.]simsekaluminyurn[.]com

Sample Domains That Contained Unique Strings Found among the IoCs

- translate[.]news
- translates[.]news
- translated[.]news
- translatenews[.]ru
- translatenews[.]org
- newstranslate[.]com
- translatednews[.]de
- translatethe[.]news
- translatenews[.]com
- translatednews[.]com
- translatednews[.]net
- news-translate[.]com
- translate-news[.]com
- newstranslated[.]com

- translate-news[.]net
- newstranslater[.]com
- utranslatenews[.]com
- newstranslate[.]info
- ektranslatednews[.]fun
- translatethenews[.]net
- translatethenews[.]com
- translateall-news[.]com
- translatenewsspeed[.]gq
- thenewstranslated[.]com
- thetranslatednews[.]com
- technologyrequest[.]ga
- technologyrequest[.]bid
- requesttechnology[.]xyz
- requesttechnology[.]org
- requesttechnology[.]net
- technologyrequest[.]com
- requesttechnology[.]com
- technologyrequest[.]life
- technology-request[.]com
- technology-requests[.]net
- requesttechnology[.]nom[.]za
- requestfortechnology[.]com
- requesttechnology[.]com[.]au
- thoughtrequest[.]technology
- technologyofferrequest[.]com
- requestintegrity[.]technology
- gdprdatarequests[.]technology
- uor-technology-request-form[.]com
- subjectaccessrequest[.]technology
- personaldatarequests[.]technology
- subjectaccessrequests[.]technology
- technologyrequestinformation[.]info
- gdprpesonaldatarequests[.]technology
- alternativeenergyrequestfortechnology[.]com
- convertremote[.]com
- protocolist[.]ru
- protocolist[.]xyz
- protocollist[.]xn--kpry57d
- protocollist[.]xn--kprw13d
- protocolist[.]com
- protocolist[.]pro
- protocollist[.]com
- protocolist[.]tech
- protocolista[.]com
- protocolist[.]site
- protocolist[.]info
- listprotocol[.]com
- protocolistas[.]es
- protocolistas[.]net
- protocol-list[.]com
- protocolistas[.]com
- protocolslist[.]com
- protocolist[.]trade
- protocolist[.]com[.]ua
- protocolist[.]online
- theprotocolist[.]com
- calistoprotocol[.]com
- listingprotocol[.]com
- holisticprotocol[.]com
- protocollist[.]website
- gettemplate[.]ir
- getemplate[.]com
- gettemplate[.]co
- gettemplate[.]us
- gettemplate[.]de
- gettemplate[.]io
- gettemplate[.]tk
- gettemplate[.]ru
- pagetemplate[.]no
- templateget[.]net
- gettemplates[.]co
- gettemplate[.]org
- gettemplate[.]net
- gettemplate[.]com
- templateget[.]com
- getemplates[.]com
- getatemplate[.]co

- getatemplate[.]ca
- gettemplates[.]ru
- get-template[.]eu
- gettemplates[.]io
- pagetemplate[.]cn
- edgetemplate[.]com
- get2template[.]com
- pagetemplates[.]de