

Cloud Atlas Navigates Us Into New Waters

 domaintools.com/resources/blog/cloud-atlas-navigates-us-into-new-waters



Executive Summary

Taking recent Cloud Atlas nameserver activity as a starting point, the DomainTools researchers enumerated a potential sinkhole network containing hundreds of previously known malicious domains spanning dozens of campaigns. Using this domain knowledge, defenders and researchers can make inferences during day-to-day analysis such as the end point of a campaign or whether or not a particular sample is still dangerous. Additionally, DomainTools researchers provide a working method for enumerating infrastructure based on nameserver activity.

Background

In the past six months, DomainTools researchers have investigated multiple campaigns from the entity known as Cloud Atlas or Inception. As mentioned prior, Cloud Atlas' targeting spans a number of government entities and industries, primarily in parts of the former Soviet Union and Europe, but has been actively seen across Asia, North America, and the Middle East as well. Cloud Atlas makes use of template injection to load malicious payloads on victim systems and spread their C2 infrastructure across a variety of cloud providers which makes tracking their activities a bit more difficult.

Nameserver Movement

On May 26, DomainTools researchers observed previously known Cloud Atlas domains transitioning their NS records from bitdomain[.]biz to one of three new nameservers that each contain roughly 150 domains that the DomainTools data science team’s risk scoring rates at a high risk for maliciousness. The original nameserver, bitdomain[.]biz, belongs to a discount hosting provider that accepts Bitcoin for payment, a common feature in APT group hosting provider choice. A number of unrelated domains exist on bitdomain[.]biz so this is not exclusive to Cloud Atlas and neither is the movement to these other nameservers.

Domain	Action	Current Server	Former Server
eurasia-research.org	Transferred	domain-imminent.com	bitdomain.biz
global-policy.org	Transferred	domain-imminent.com	bitdomain.biz
ms-update.org	Transferred	domain-transition1.com	bitdomain.biz
msofficeupdate.org	Transferred	domain-transition1.com	bitdomain.biz
newupdate.org	Transferred	newregs-domain.com	bitdomain.biz
wordupdate.org	Transferred	newregs-domain.com	bitdomain.biz

The movement between nameservers can be indicative of a number of things, but first and foremost movement means that there was interaction with the domain as someone or some process had to change the record. Many malicious domains, after use, are left to become stale but a domain moving between nameservers indicates that there is another intent left for that domain. This could be the final steps in a well organized campaign’s cleanup process, a further aging of the domain for other campaigns in the future, or movement to other infrastructure for a myriad reasons.

Since these domains are each less than 100 days old, they have not yet expired on their original registration, so this isn’t a “drop catch” situation. These nameservers also do not belong to any sinkholes that DomainTools researchers are aware of at this time. Lastly, the two-by-two pairing seems like an odd pattern since one would assume sinkhole infrastructure would keep domains from the same campaign on the same servers for measuring telemetry.

Examining New Nameservers

The domains behind these new nameservers, which Cloud Atlas has not previously been seen using, are well aged between the three of them with over five and a half years for an average age. With youth being a heavy indicator in maliciousness prediction products across the cyber threat intelligence industry, many threat actors have begun turning to well aged domain reseller services or trying to catch domains that have recently dropped from their registration. A prime example of this could be the avsvmcloud[.]com domain used in the high-profile SolarWinds supply chain compromise earlier this year. In this case, we have a long, contiguous set of ownership records in historical Whois for the domains attached to these nameservers so none of the above possibilities seem to fit here.

Domain	Status	Create Date	Expiration Date	Name Server	IP
<input type="checkbox"/> domain-imminent.com Inactive 4,090 days old 10 years ago Inspect Inactive 1 Guided Pivot	Inactive	2010-03-15	2011-03-15	Hostname ns63.domaincontrol.com ns64.domaincontrol.com	IP Information IP: 68.178.232.99 ISP IP Information: GoDaddy.com LLC ASN: 26496 Country Code: US
<input type="checkbox"/> domain-transition1.com Active 1,010 days old in 3 months Inspect 3 Guided Pivots	Active	2018-08-20	2021-08-20	Hostname ns1.domain-transition1.com ns2.domain-transition1.com	IP Information IP: 35.168.154.15 ISP IP Information: Amazon Technologies Inc. ASN: 14618 Country Code: US
<input type="checkbox"/> newregs-domain.com Active 974 days old in 4 months Inspect 3 Guided Pivots	Active	2018-09-25	2021-09-25	Hostname ns1.newregs-domain.com ns2.newregs-domain.com	IP Information IP: 35.169.140.232 ISP IP Information: Amazon Technologies Inc. ASN: 14618 Country Code: US

The top IP address looks to belong to a domain parking provider that has been around since 2010. However, the bottom two addresses point to Amazon EC2 nodes that are running just DNS services on port 53, acting as a DNS forwarding service -- a sign this may be an unknown sinkhole. Digging into a history of domains that have resided on these nameservers ties them to other maliciousness, such as the .NET RAT SamoRAT's domain samorat[.]com which resides on newregs-domain[.]com until May 19, 2021 or the domain 360mediashare[.]com seen distributing another RAT via phishing emails in late 2020. In fact, the same goes for the domain-transition1[.]com nameserver which hosts domains such as porkhalal[.]site which the Zusy banking trojan has been observed using for C2 and alhajikudi[.]com which has been observed in traffic of other malware samples in early 2021.

As DomainTools researchers looked further into these nameservers and the domains contained on them, it became apparent that this must be a domain reseller network or a sinkhole telemetry network due to the large swath of known malicious domains transitioning through these nameservers over time. DomainTools' own proximity risk scoring rated all of these related domains an average of 80 due simply to their proximity to known malicious infrastructure on industry standard blocklists. Typically, in the experience of DomainTools researchers, a scoring above 70 means that a domain should not be trusted and should be investigated further. It became apparent that mapping this network would be a useful exercise.

Looking For More Nameservers

With these bottom two domains there is a pattern we can treat as a composite object for hunting additional infrastructure:

- They have nameservers that are hosted on the domain themselves.
- This domain is hosted on Amazon's AWS on an EC2 node.
- The domain contains a dash.

- The emails in the Whois record have both privacyprotect[.]org and bigrock[.]com in the record.

Searching for these features in the [DomainTools Iris Investigate](#) data set reveals a total of 5 additional domains that DomainTools researchers can say with high confidence belong to the same clustering:

Domain	Name Server	IP														
<input type="checkbox"/> domain-transition.com <input type="button" value="Inspect"/> 3 Guided Pivots	<table border="1"> <thead> <tr> <th>Hostname</th> <th>IP Information</th> </tr> </thead> <tbody> <tr> <td>ns1.domain-transition.com</td> <td>34.206.177.175</td> </tr> <tr> <td>ns2.domain-transition.com</td> <td>34.206.177.175</td> </tr> </tbody> </table>	Hostname	IP Information	ns1.domain-transition.com	34.206.177.175	ns2.domain-transition.com	34.206.177.175	<table border="1"> <thead> <tr> <th>IP</th> <th>ISP IP Information</th> <th>ASN</th> <th>Country Code</th> </tr> </thead> <tbody> <tr> <td>34.206.177.175</td> <td>Amazon Technologies Inc.</td> <td>14618</td> <td>US</td> </tr> </tbody> </table>	IP	ISP IP Information	ASN	Country Code	34.206.177.175	Amazon Technologies Inc.	14618	US
Hostname	IP Information															
ns1.domain-transition.com	34.206.177.175															
ns2.domain-transition.com	34.206.177.175															
IP	ISP IP Information	ASN	Country Code													
34.206.177.175	Amazon Technologies Inc.	14618	US													
<input type="checkbox"/> domain-transition2.com <input type="button" value="Inspect"/> 3 Guided Pivots	<table border="1"> <thead> <tr> <th>Hostname</th> <th>IP Information</th> </tr> </thead> <tbody> <tr> <td>ns1.domain-transition2.com</td> <td>52.22.100.42</td> </tr> <tr> <td>ns2.domain-transition2.com</td> <td>52.22.100.42</td> </tr> </tbody> </table>	Hostname	IP Information	ns1.domain-transition2.com	52.22.100.42	ns2.domain-transition2.com	52.22.100.42	<table border="1"> <thead> <tr> <th>IP</th> <th>ISP IP Information</th> <th>ASN</th> <th>Country Code</th> </tr> </thead> <tbody> <tr> <td>52.22.100.42</td> <td>Amazon Technologies Inc.</td> <td>14618</td> <td>US</td> </tr> </tbody> </table>	IP	ISP IP Information	ASN	Country Code	52.22.100.42	Amazon Technologies Inc.	14618	US
Hostname	IP Information															
ns1.domain-transition2.com	52.22.100.42															
ns2.domain-transition2.com	52.22.100.42															
IP	ISP IP Information	ASN	Country Code													
52.22.100.42	Amazon Technologies Inc.	14618	US													
<input type="checkbox"/> domain-transition3.com <input type="button" value="Inspect"/> 3 Guided Pivots	<table border="1"> <thead> <tr> <th>Hostname</th> <th>IP Information</th> </tr> </thead> <tbody> <tr> <td>ns1.domain-transition3.com</td> <td>34.236.128.239</td> </tr> <tr> <td>ns2.domain-transition3.com</td> <td>34.236.128.239</td> </tr> </tbody> </table>	Hostname	IP Information	ns1.domain-transition3.com	34.236.128.239	ns2.domain-transition3.com	34.236.128.239	<table border="1"> <thead> <tr> <th>IP</th> <th>ISP IP Information</th> <th>ASN</th> <th>Country Code</th> </tr> </thead> <tbody> <tr> <td>34.236.128.239</td> <td>Amazon Technologies Inc.</td> <td>14618</td> <td>US</td> </tr> </tbody> </table>	IP	ISP IP Information	ASN	Country Code	34.236.128.239	Amazon Technologies Inc.	14618	US
Hostname	IP Information															
ns1.domain-transition3.com	34.236.128.239															
ns2.domain-transition3.com	34.236.128.239															
IP	ISP IP Information	ASN	Country Code													
34.236.128.239	Amazon Technologies Inc.	14618	US													
<input type="checkbox"/> domains-green.com <input type="button" value="Inspect"/> 3 Guided Pivots	<table border="1"> <thead> <tr> <th>Hostname</th> <th>IP Information</th> </tr> </thead> <tbody> <tr> <td>ns1.domains-green.com</td> <td>18.210.70.61</td> </tr> <tr> <td>ns2.domains-green.com</td> <td>18.210.70.61</td> </tr> </tbody> </table>	Hostname	IP Information	ns1.domains-green.com	18.210.70.61	ns2.domains-green.com	18.210.70.61	<table border="1"> <thead> <tr> <th>IP</th> <th>ISP IP Information</th> <th>ASN</th> <th>Country Code</th> </tr> </thead> <tbody> <tr> <td>18.210.70.61</td> <td>Amazon Technologies Inc.</td> <td>14618</td> <td>US</td> </tr> </tbody> </table>	IP	ISP IP Information	ASN	Country Code	18.210.70.61	Amazon Technologies Inc.	14618	US
Hostname	IP Information															
ns1.domains-green.com	18.210.70.61															
ns2.domains-green.com	18.210.70.61															
IP	ISP IP Information	ASN	Country Code													
18.210.70.61	Amazon Technologies Inc.	14618	US													
<input checked="" type="checkbox"/> suspended-domians.com <input type="button" value="Inspect"/> 3 Guided Pivots	<table border="1"> <thead> <tr> <th>Hostname</th> <th>IP Information</th> </tr> </thead> <tbody> <tr> <td>ns1.suspended-domians.com</td> <td>18.211.139.57</td> </tr> <tr> <td>ns2.suspended-domians.com</td> <td>18.211.139.57</td> </tr> </tbody> </table>	Hostname	IP Information	ns1.suspended-domians.com	18.211.139.57	ns2.suspended-domians.com	18.211.139.57	<table border="1"> <thead> <tr> <th>IP</th> <th>ISP IP Information</th> <th>ASN</th> <th>Country Code</th> </tr> </thead> <tbody> <tr> <td>18.211.139.57</td> <td>Amazon Technologies Inc.</td> <td>14618</td> <td>US</td> </tr> </tbody> </table>	IP	ISP IP Information	ASN	Country Code	18.211.139.57	Amazon Technologies Inc.	14618	US
Hostname	IP Information															
ns1.suspended-domians.com	18.211.139.57															
ns2.suspended-domians.com	18.211.139.57															
IP	ISP IP Information	ASN	Country Code													
18.211.139.57	Amazon Technologies Inc.	14618	US													

Note the misspelling in suspended-domians[.]com. Expanding on these nameservers reveals just over 1,086 domains, most of which have been involved in some sort of cybercrime activity in the past. Of those 1,086 domains none of them had a reseller page when navigating to the domain which domain resale companies use to signal that the domain is for sale. Lastly, DomainTools Research noticed that all of the domains associated with those nameservers pointed to one of 3 IP addresses, spread across all nameservers, that definitively tied this clustering together.

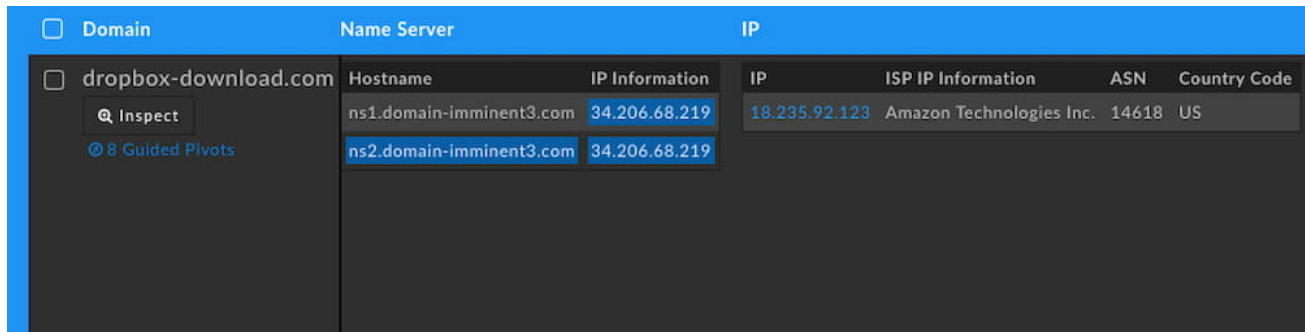
IPs of Nameserver Cluster

18.235.92[.]123

50.17.5[.]224

54.227.98[.]220

Inverting the search from nameserver properties to solely A records reveals a single site as an outlier: dropbox-download[.]com. It is an outlier because it contains a different nameserver in domain-imminent3[.]com, a naming schema nearly identical to one of the nameservers associated with the original Cloud Atlas movement at the beginning of this report, domain-imminent[.]com. Of note is that the dropbox-download[.]com domain here is associated with [TA505](#), the group behind the [Dridex](#) banking trojan, from a campaign they ran over two years ago.



The screenshot shows a table with columns: Domain, Name Server, and IP. The domain 'dropbox-download.com' is selected, and its nameservers are listed. The IP address 18.235.92.123 is highlighted, and its ISP information is shown as Amazon Technologies Inc. with ASN 14618 and Country Code US. The other nameservers are ns1.domain-imminent3.com and ns2.domain-imminent3.com, both with IP 34.206.68.219.

Domain	Name Server	IP
dropbox-download.com	ns1.domain-imminent3.com	34.206.68.219
	ns2.domain-imminent3.com	34.206.68.219
		18.235.92.123

ISP IP Information: Amazon Technologies Inc. 14618 US

Viewing all domains on domain-imminent3[.]com, repeating the process from above, reveals another common IP address (52.6.206[.]192) spanning multiple new nameservers including domain-imminent1[.]com, domain-imminent2[.]com. The inclusion of these final two nameservers contain a recent lapse in privacy protection on the Whois record and an email address of resellerclub@protonmail[.]com that is tied to them.

Inspect: domain-imminent1.com

Domain Profile Screenshot History **Whois History** Hosting History SSL Profile

Historical Records
16 records found

< Older 2021-05-26 - (a day ago) Newer >


> 2021-05-26	changes	Domain	domain-imminent1.com
2021-03-31	changes	Record Date	2021-05-26
2021-03-25	changes	Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
2020-11-26	changes	Server	whois.publicdomainregistry.com
2020-11-12	changes	Created	2018-12-13 (2 years ago)
2020-08-11	changes	Updated	2020-08-26 (9 months ago)
2020-05-10	changes	Expires	2021-12-13 (in 7 months)
2020-02-05	changes	Unique Emails	<ul style="list-style-type: none"> abuse-contact@publicdomainregistry.com resellerclub@protonmail.com
2020-01-23	changes	View Changes	<ul style="list-style-type: none"> Stub by Side Initial Raw Records
2019-12-15	changes	<pre> Domain Name: DOMAIN-IMMINENT1.COM Registry Domain ID: 2342843937_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2021-01-18T12:52:18Z Creation Date: 2018-12-13T10:27:49Z Registrar Registration Expiration Date: 2021-12-13T10:27:49Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 383 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Proton Registrant Organization: Protonmail Registrant Street: mumbai Registrant City: Mumbai Registrant State/Province: Maharashtra Registrant Postal Code: 400067 Registrant Country: IN Registrant Phone: +91.1231451212 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: resellerclub@protonmail.com Registry Admin ID: Not Available From Registry Admin Name: Proton Admin Organization: Protonmail Admin Street: mumbai Admin City: Mumbai Admin State/Province: Maharashtra Admin Postal Code: 400067 Admin Country: IN Admin Phone: +91.1231451212 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: resellerclub@protonmail.com Registry Tech ID: Not Available From Registry Tech Name: Proton Tech Organization: Protonmail </pre>	
2019-11-02	changes		
2019-08-01	changes		
2019-06-13	changes		
2019-03-15	changes		
2018-12-14	changes		
2018-12-13	changes		

Ok

This email in historical Whois records ties to 20 records total that span most of the nameservers DomainTools researches enumerated. On top of that, many of the domains in that group—including elsewhere in the list of total domains—move to the nameservers at foundationapi[.]com at one point or another, a property of Endurance International Group, a company in the domain and web services space that owns a number of properties including BigRock, HostGator, and ResellerClub.

Domain	foundationapi.com
Record Date	2021-05-26
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Server	whois.publicdomainregistry.com
Created	2001-10-27 (20 years ago)
Updated	2020-07-07 (a year ago)
Expires	2021-10-27 (in 5 months)
Unique Emails	<ul style="list-style-type: none">• abuse-contact@publicdomainregistry.com• corpdomains@endurance.com

ResellerClub allows for the bulk resale of domains. Searching on their documentation you can see the use of foundationapi[.]com as a backend as well as the services and pricing they offer for bulk domain purchases.



Dear Reseller,

In this mail we will be covering notifications with regards to -

- [Pricing Bands now Live!](#)
- [IP Restrictions for the SOAP API](#)
- [DNS Management available via the API](#)
- [Change in Whois details of Privacy Protected Domains](#)

Pricing Bands now Live!

Pricing bands are now live. Kindly login and modify your pricing, if necessary.

For more details on pricing bands and the impact of this launch, please refer to our previous mail: http://resources.resellerclub.com/mailers/price_bands_20-12-10.html

IP Restrictions for the SOAP API

Like the HTTP API, we have now introduced IP restrictions on the SOAP API. API users will be required to modify their Host URLs before **10th February, 2011**.

Changes Required:

For example, if you are using a URL like -

<https://www.foundationapi.com/anacreon/servlet/APIv3>
or
<http://www.foundationapi.com/anacreon/servlet/APIv3>

You will need to change it to -

<https://soapapi.com/anacreon/servlet/APIv3>
or
<http://soapapi.com/anacreon/servlet/APIv3> respectively.

Important:

You will need to white-list your IP address in the Control Panel to continue using the API. The details of how you can do this are given here:

http://manage.resellerclub.com/kb/answer/744#heading_2

We will deprecate the old URLs on the **10th of February, 2011**, so please make the required changes before the deadline.

DNS Management available via the API

The DNS Service that we offer free with every Domain is now available through the API.

The complete API documentation is available at:

<http://manage.resellerclub.com/kb/answer/1091>

Change in the Whois details of Privacy Protected Domains

We have modified the Whois details of our Free Privacy Protect Service.

The new details are available at: <http://privacyprotect.org/about-privacyprotection/>

Domain Extension	Price 1	Price 2
.eu	\$2.49	\$7.99
.co	\$9.49	\$24.99
.online	\$6.99	\$30.99
.top	\$7.99	
.CLUB	\$1.99	\$10.99

The Domain Swamp

Expanding across the domains tied to all nameservers there are a total of 1,378 domains, 559 of which are on known industry blocklists for malware and on average score above 80 in the DomainTools Risk Score engine. Going through those 1,378 domains, none could be found on domain auction sites or for sale, so this further backs up the potential that this is a sinkhole network run by the Endurance International Group or one of their subsidiaries. To show the broad swath of domains and campaigns associated, DomainTools researchers coupled one nameserver's holdings, domain-imminent1[.]com, with Alienvault OTX pulses below.

Domain	Associated Campaign
1999beats[.]com	<u>Ryuk Ransomware</u>
401kplansinfo[.]com	
aahnaturals[.]net	<u>Ryuk Ransomware</u> , <u>Emotet</u>
acquistic[.]space	
adguard[.]name	<u>FIN7 Carbanak</u>

Domain	Associated Campaign
adwordsgooglee[.]website	
agenziainformazioni[.]jicu	<u>Maze Ransomware</u>
amadiohaowo[.]com	<u>Miscellaneous Activity</u>
anonymous-sec[.]com	<u>AZORult</u>
anz-payments[.]com	
babstefbab[.]com	<u>Dimnie</u>
babtrabbab[.]biz	<u>Dimnie</u>
balkher[.]eu	<u>SLoad</u>
bdsnhatnam[.]info	<u>Ryuk Ransomware</u> , <u>Emotet</u>
berjaya88[.]net	<u>Ryuk Ransomware</u> , <u>Emotet</u>
bigbluepay[.]com	<u>Ryuk Ransomware</u>
brahmanimetal[.]com	<u>Ryuk Ransomware</u> , <u>Emotet</u>
corn-en-us[.]com	<u>DarkBasin</u>
dixii[.]org	
download-365[.]com	<u>XDSpy</u>
dweandro[.]com	<u>Salfram</u>
eitivo[.]com	
electronic-messagecom[.]com	<u>Banload</u>
eltta[.]host	
feltongexp[.]com	<u>AZORult</u>
firstbankhome[.]com	<u>Racoon</u>
gccorsp[.]com	<u>Miscellaneous Activity</u>
green0green[.]com	<u>AZORult</u>
grnaeil[.]com	<u>APT37</u>
help-covid[.]com	<u>Covid Phisting US-CERT</u>

Domain	Associated Campaign
hictip[.]com	<u>Miscellaneous Activity</u>
igjqwnedjgqwnqwemnta[.]net	<u>Miscellaneous Activity</u>
indopet[.]site	
issth[.]com	<u>Miscellaneous Activity</u>
jjsmiths[.]com	<u>Miscellaneous Activity</u>
lanadlite[.]com	<u>LokiBot</u>
lesehanpelangi[.]com	<u>Miscellaneous Activity</u>
lflalallalaakaka[.]com	
lgjasjdnqwtjasjsadasd[.]net	
littlebarbar[.]online	<u>AZORult</u>
loadmanager07[.]com	<u>AZORult</u>
lookper[.]eu	<u>Kimsuky</u>
loxliver[.]com	<u>Ryuk</u>
maleass[.]eu	<u>sLoad/Ramnit</u>
managementdirector[.]com	<u>APT33</u>
marcussoil[.]com	
mobile-signin1[.]com	
mountasd[.]com	<u>Ryuk</u>
nrevig[.]host	<u>IcedID</u>
officelog[.]org	<u>AZORult</u>
out-look-mail-bh[.]com	<u>Bahamut</u>
panunltd[.]co.uk	
pharma--partners[.]com	
piavee[.]com	<u>Miscellaneous Activity</u>
pilsans[.]com	<u>AZORult</u>

Domain	Associated Campaign
platinet-pl[.]com	<u>Pony</u>
puckhunterror[.]com	<u>Ryuk</u>
rakeeerrrrrrrr[.]xyz	<u>AZORult</u>
randomware01[.]info	<u>Win32.MereTam</u>
reasgt[.]me	
regabok[.]eu	
relkur[.]eu	
sakural[.]co.uk	
savarsineklik[.]com	<u>Miscellaneous Activity</u>
secure-mobile1[.]com	<u>Observed Phishing</u>
selftasarim[.]com	<u>AZORult</u>
sign-id[.]us	<u>Miscellaneous Activity</u>
spark-login[.]com	<u>Miscellaneous Activity</u>
stepsaweb[.]com	<u>Miscellaneous Activity</u>
systemltd[.]link	<u>Win32.Grimagent</u>
sznamuip[.]com	<u>Miscellaneous Activity</u>
thelucy[.]top	
thernagictouch[.]com	<u>LokiBot</u>
tobocoq[.]com	<u>Miscellaneous Activity</u>
update-flashes[.]com	<u>APT32</u>
webuserinfo[.]com	<u>Kimsuky</u>
wefyourfwggggg[.]com	
worldupdate[.]live	<u>Donot Group</u>
ytilac[.]pw	<u>Miscellaneous Activity</u>

Conclusion

At this point DomainTools researchers are led to believe that these nameservers are a holding pen for known malicious domains on the reseller network until they can be resold or are actively being used as a sinkhole by the reseller network for telemetry. Since DomainTools researchers cannot find a description of the sinkhole network or any of that telemetry being posted elsewhere online, defenders can only assume that this is a private sinkhole network associated with Endurance.

Lessons for Defenders

If you are an analyst working with malicious software or mapping adversary infrastructure, knowing of these dead zones in domain data so that you do not get distracted by them when trying to map live infrastructure is key to efficiently researching threats. For threat hunters, watching the transitioning of domains on and off these nameservers, through a tool like the [DomainTools Nameserver Monitor](#), can provide ample domains for hunting queries on public repositories of malicious binaries and lead to pivots of fresh, un-sinkholed infrastructure.

Nameserver List

domain-imminent[.]com

domain-imminent1[.]com

domain-imminent2[.]com

domain-imminent3[.]com

domain-transition1[.]com

domain-transition2[.]com

domain-transition3[.]com

domains-green[.]com

suspended-domians[.]com

newregs-domain[.]com

Iris Search Hash for All Domains On These Nameservers:

U2FsdGVkX19inpzBsHU8tDBrjLPfcJTcmLc+013CCJpuRlnDdlUogNF5k0NIqexu04v7Gki1kMrvqup8FVTtM