

Finding AnchorDNS C2s With Iris Investigate

 domaintools.com/resources/blog/finding-anchordns-c2s-with-iris-investigate



Executive Summary

Taking Kryptos Logic's initial report, DomainTools Researchers illustrate how to hunt for AnchorDNS C2s in infrastructure data with a combination of passive DNS and infrastructure observables for identifying those C2s accurately. Through this process they uncover an additional four C2 domains not found in the initial reporting.

Background on AnchorDNS

AnchorDNS is a backdoor most commonly used by [TrickBot](#) when going after their most prized victims. As an exfiltration tool, AnchorDNS uses DNS for C2 communications as well as exfiltration of data. This remains highly effective as most organizations do not filter their outbound DNS traffic.

Last week the researchers at Kryptos Logic published an [article](#) on recent changes to AnchorDNS and a new tool dubbed Anchor Adjuster that allows the attackers using the exfiltration tool to adjust the configuration on the fly for further evasion. Along with this tool comes a change in the way that the malware communicates with the C2 as well as new encoding that makes detection more difficult. This is all run from [Cobalt Strike](#), the commercial tool loved by so many threat actors operating today.

Hunting AnchorDNS

Kryptos Logic provides an excellent breakdown of the changes in operation along with a fully detailed write up of the various queries and responses that's worth reading if you are a defender looking into these samples. Through their analysis of the samples, Kryptos Logic found the following set of C2 domains:

farfaris[.]com

kalarada[.]com

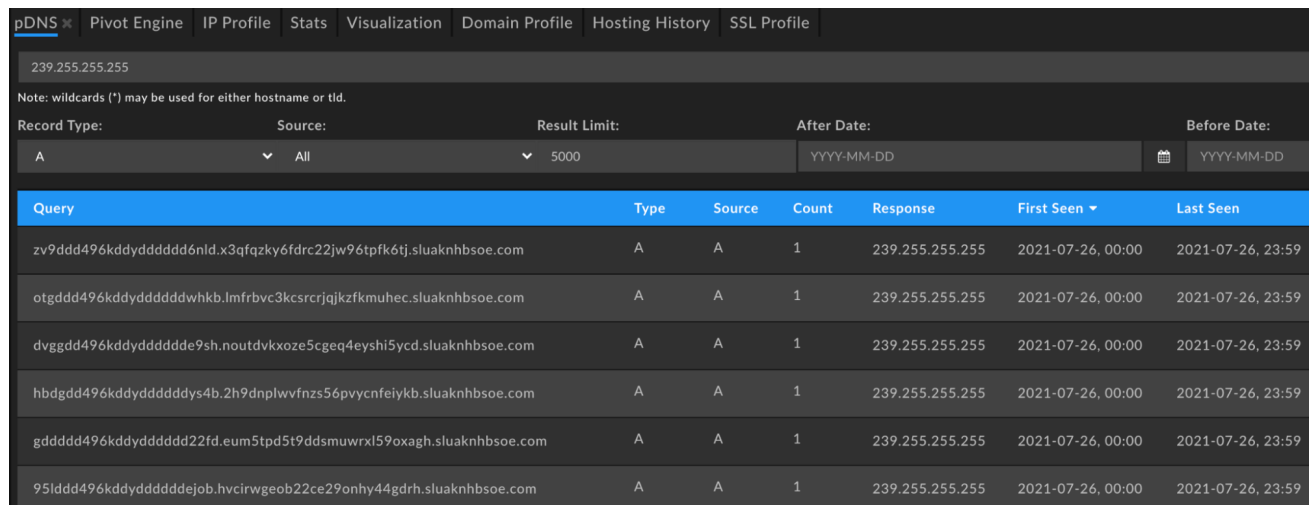
xyskencevli[.]com

sluaknhbsoe[.]com

jetbiokleas[.]com

nyhglaksa[.]com

Looking for ways to detect new C2s through our daily scanning of the Internet, DomainTools Researchers noticed an interesting change when reading this report that we will pivot on: the sleep and retry response from the C2. When an AnchorDNS C2 receives a bot's command successfully, the C2 responds with its own IP address. Additionally, when the C2 is unable to respond the response will be 239.255.255[.]255 which tells the bot to sleep for the configured amount of time and retry again later. Typically, addresses under 224.0.0.0/4 are reserved for Multicast and shouldn't be seen in a DNS response in this way. This makes looking for them in passive DNS and subsequently verifying the resulting domains based on their query labels matching the AnchorDNS encoding scheme rather trivial.



Query	Type	Source	Count	Response	First Seen	Last Seen
zv9ddd496kddydddd6nld.x3qfzky6fdr22jw96tpfk6tj.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59
otgddd496kddyddddwhkb.lmfrbvc3kcsrjzkzfkmuhec.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59
dvggdd496kddyddddde9sh.noutdvkxoze5cgeq4eyshi5ycd.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59
hbdgdd496kddydddddys4b.2h9dnplwvfnzs56pvycnfeiykb.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59
gddddd496kddydddd22fd.eum5tpd5t9ddsmuwxl59oxagh.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59
95lddd496kddydddddejob.hvcirwgeob22ce29onhy44gdrh.sluaknhbsoe.com	A	A	1	239.255.255.255	2021-07-26, 00:00	2021-07-26, 23:59

Due to the encoding scheme there ends up being a lot of noise in these queries. In fact, if we query Farsight passive DNS alone for the number of results that match our query within the time frame that this AnchorDNS variant has been active we see over 130,000 query and response pairs.

Time First Seen ↕	Time Last Seen ↕	Count	Number of Results
2020-12-23 14:08:06	2021-06-02 16:17:18	201627	136976

To reduce the noise we can filter these by just the second-level domain (SLD). Iris Investigate does this automatically for you with the “Send Domains to Pivot Engine” button in the bottom-right of the passive DNS interface. Once in the Pivot Engine there are a number of new potential C2 domains:

limeal[.]com

muncuc[.]com

newarg[.]com

tuxomibo[.]com

If we examine those domains alongside the known domains from the original Kryptos Logic report, we see that the known domains are already scored by the DomainTools Risk Score engine as 100 or already on a blacklist. The other new C2 domains are in varying states of risk, some high enough to be alarming and others flying under the radar entirely.

Domain	Tags	Risk Score	Email	Email Domain												
limeal.com	<input type="checkbox"/> Inspect 2 Guided Pivots	80	<table border="1"> <thead> <tr> <th>Address</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com</td> <td>Admin</td> </tr> <tr> <td>hostmaster@registrar-servers.com</td> <td>DNS/SOA</td> </tr> <tr> <td>50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com</td> <td>Registrant</td> </tr> <tr> <td>50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com</td> <td>Technical</td> </tr> <tr> <td>abuse@namecheap.com</td> <td>Whois</td> </tr> </tbody> </table>	Address	Type(s)	50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Admin	hostmaster@registrar-servers.com	DNS/SOA	50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Registrant	50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Technical	abuse@namecheap.com	Whois	namecheap.com registrar-servers.com withheldforprivacy.com
Address	Type(s)															
50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Admin															
hostmaster@registrar-servers.com	DNS/SOA															
50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Registrant															
50718681aea94cf7bb9e95ed236222d8.protect@withheldforprivacy.com	Technical															
abuse@namecheap.com	Whois															
muncuc.com	<input type="checkbox"/> Inspect	13	<table border="1"> <thead> <tr> <th>Address</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>dns@openprovider.eu</td> <td>DNS/SOA</td> </tr> <tr> <td>abuse@registrar.eu</td> <td>Whois</td> </tr> </tbody> </table>	Address	Type(s)	dns@openprovider.eu	DNS/SOA	abuse@registrar.eu	Whois	openprovider.eu registrar.eu						
Address	Type(s)															
dns@openprovider.eu	DNS/SOA															
abuse@registrar.eu	Whois															
newarg.com	<input type="checkbox"/> Inspect 3 Guided Pivots	56	<table border="1"> <thead> <tr> <th>Address</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com</td> <td>Admin</td> </tr> <tr> <td>hostmaster@registrar-servers.com</td> <td>DNS/SOA</td> </tr> <tr> <td>3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com</td> <td>Registrant</td> </tr> <tr> <td>3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com</td> <td>Technical</td> </tr> <tr> <td>abuse@namecheap.com</td> <td>Whois</td> </tr> </tbody> </table>	Address	Type(s)	3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Admin	hostmaster@registrar-servers.com	DNS/SOA	3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Registrant	3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Technical	abuse@namecheap.com	Whois	namecheap.com registrar-servers.com withheldforprivacy.com
Address	Type(s)															
3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Admin															
hostmaster@registrar-servers.com	DNS/SOA															
3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Registrant															
3937284c0ea04f379babe59dd2e78b55.protect@withheldforprivacy.com	Technical															
abuse@namecheap.com	Whois															
nyhgloksa.com	<input type="checkbox"/> Inspect	100	<table border="1"> <thead> <tr> <th>Address</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>abuse@registrar.eu</td> <td>Whois</td> </tr> </tbody> </table>	Address	Type(s)	abuse@registrar.eu	Whois	registrar.eu								
Address	Type(s)															
abuse@registrar.eu	Whois															

Additional Observations

Since DomainTools researchers like to treat all indicators of compromise (IoCs) as composite objects, there are a few other elements outside of just the noise and construction of the query and response pairs found in passive DNS that make up this C2 infrastructure that could be used in hunting for C2s in the future. These additional elements are important because they are fundamental in how these new samples work to make up a more robust method for identifying this infrastructure.

The oldest domain in this set that matches our profile is muncuc[.]com and comes in at just less than a year old with records up to the time of this writing. This tells us that when hunting for these result sets, researchers can time box to the last year when looking for new C2 infrastructure and that older infrastructure remains active.

Next, there is the use of a varied number of hosting providers but there are overlaps in ColoCrossing (AS36532), Green Floid (AS50979), and Owned-Networks (AS40676). This shows a preference that can be used to narrow down potential detections before moving further up the Pyramid of Pain and analyzing a sample to discover the specific, custom encoding for the DNS queries.

Lastly, the IP of the A record is the same as the IP of the two NS records which point to ns1.[domain].com and ns2.[domain].com. This makes sense and is a requirement for malicious infrastructure performing DNS tunneling. Without control of the nameservers the attackers could not have the additional logic required to parse and respond to messages with commands. In fact, this is often a quick indicator that a domain is malicious as most legitimate groups opt to outsource their DNS infrastructure these days to a number of different cloud services that make management easy and programmatic.

Takeaways

Data sets such as passive DNS are ideal for hunting for C2 communications that leverage DNS for exfiltration due to the sheer number of query and response pairs required by the attacker. While this data is available in public data sets like the four passive DNS providers in DomainTools Iris Investigate, a similar setup using free and open source tools such as CIRCL's d4 Project can be useful for passively monitoring the DNS queries in your own infrastructure and useful for revealing malicious software operating over passive DNS.

Additionally, domain data found in Iris Investigate is useful for further verification of any domains which surface as potential C2 communication. Attackers have to control the entirety of a nameserver for DNS exfiltration and signaling so NS records for C2 domains are an always useful signal in determining the intent of a domain.

Iris Hash Containing All Known C2s

U2FsdGVkX19QbpKjLRpwXzsMlso1XaIChMZoKECwCmCkCtr06hGK0ginsvV/j sBNnd5fNML2H0cDz0GBqdRkX