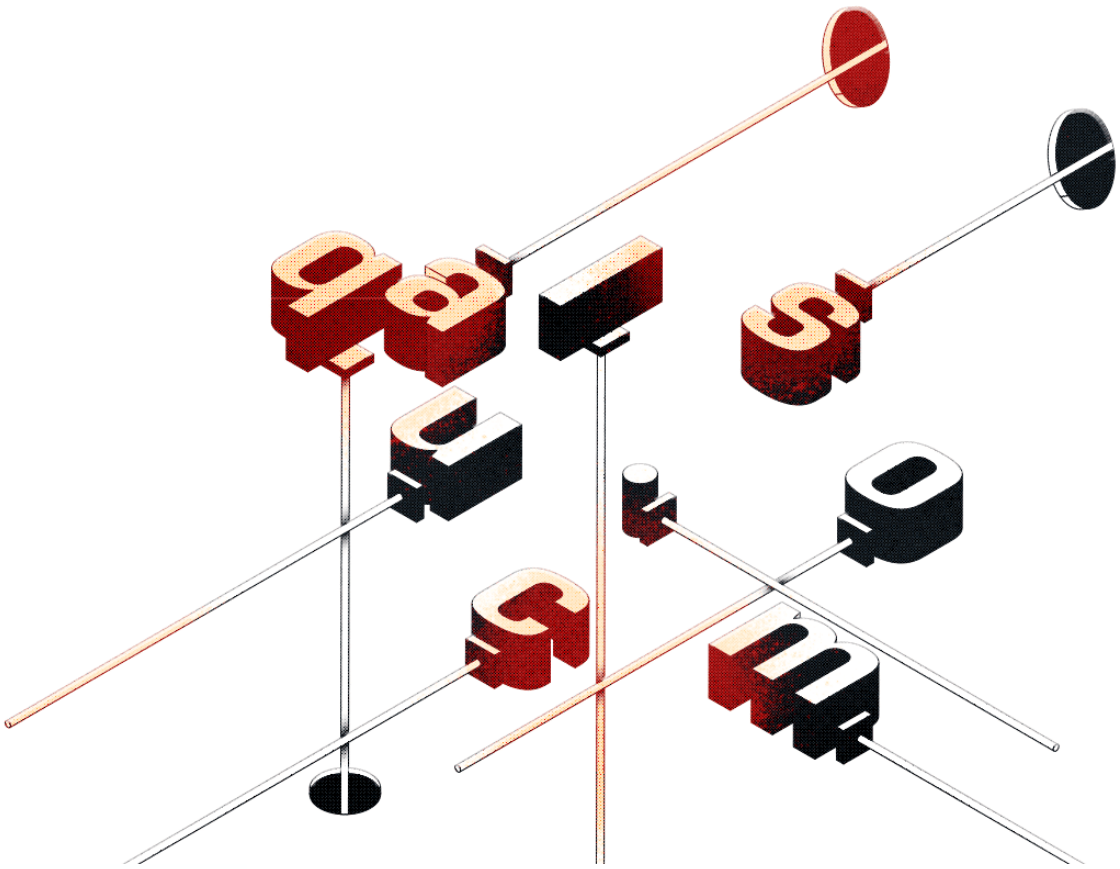
The DGA Algorithm Used by Dealply and Bujo Campaigns

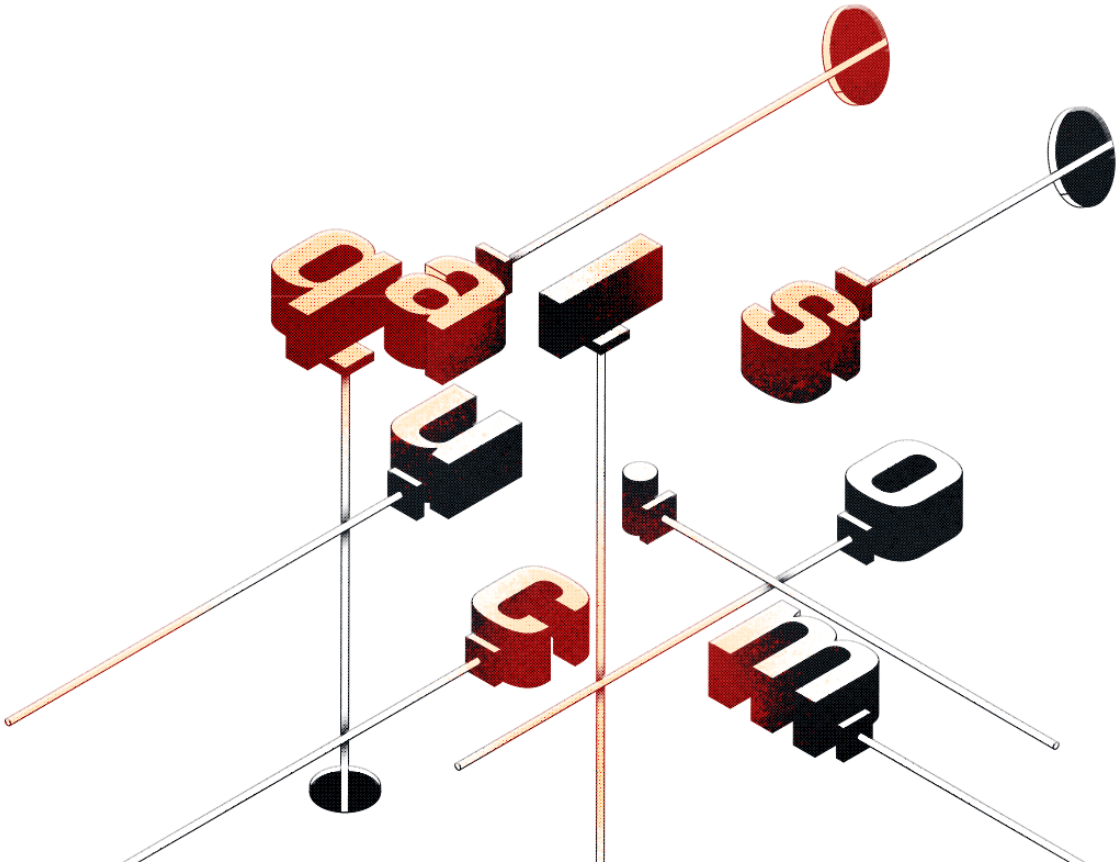
catonetworks.com/blog/the-dga-algorithm-used-by-dealply-and-bujo/

March 1, 2022



Elad Menahem

March 1, 2022
5m read



Listen to post:

During a recent malware hunt[1], the Cato research team identified some unique attributes of DGA algorithms that can help security teams automatically spot malware on their network.

The “Shimmy” DGA

DGAs (Domain Generator Algorithms) are used by attackers to generate a large number of – you guessed it – domains often used for C&C servers. Spotting DGAs can be difficult without a clear, searchable pattern.

Cato researchers began by collecting traffic metadata from malicious Chrome extensions to their C&C services. Cato maintains a data warehouse built from the metadata of all traffic flows crossing its global private backbone. We analyze those flows for suspicious traffic to hunt threats on a daily basis.

The researchers were able to identify the same traffic patterns and network behavior in traffic originating from 80 different malicious Chrome extensions, which were identified as from the Bujo, Dealply and ManageX families of malicious extensions. By examining the C&C domains, researchers observed an algorithm used to create the malicious domains. In many cases, DGAs appear as random characters. In some cases, the domains contain numbers, and in other cases the domains are very long, making them look suspicious.

Here are a few examples of the C&C domains (full domain list at the end of this post):

qalus.com	jurokotu.com	bunafo.com	naqodur.com	womohu.com	bosojojo.com
mucac.com	kuqotaj.com	bunupoj.com	pocakaqu.com	wuqah.com	dubocoso.com
sanaju.com	lufacam.com	cajato.com	qunadap.com	dagaju.com	fupoj.com

The most obvious trait the domains have in common is that they are all part of ".com" TLD (Top-Level Domain). Also, all the prefixes are five to eight letters long.

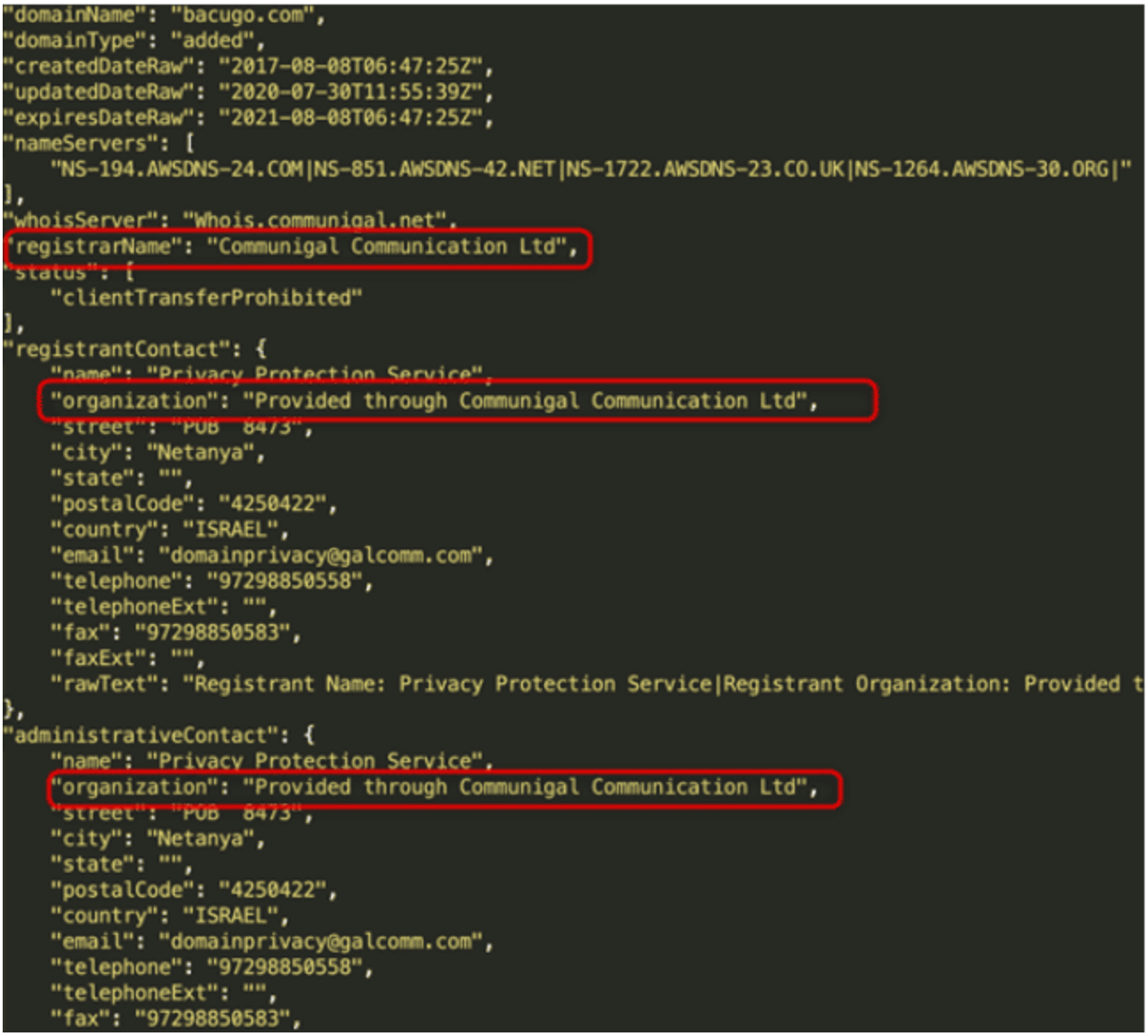
There are other factors shared by the domains. For one, they all start with consonants and then create a pattern that is built out of consonants and vowels; so that every domain is represented by consonant + vowel + consonant + vowel + consonant, etc. As an example, in jurokotu.com domain, removing the TLD will bring "jurokotu", and coloring the word to consonants (red) and vowels (blue) will show the pattern: "jurokotu".

From the domains we collected, we could see that the adversaries used the vowels: o, u and a, and consonants: q, m, s, p, r, j, k, l, w, b, c, n, d, f, t, h, and g. Clearly, an algorithm has been used to create these domains and the intention was to make them look as close to real words as possible.

"Shimmy" DGA infrastructure

A few additional notable findings are related to the same common infrastructure used by all the C&C domains.

All domains are registered using the same registrar – Gal Communication (CommuniGal) Ltd. (GalComm), which was previously associated with registration of malicious domains [2].



The domains are also classified as ‘uncategorized’ by classification engines, another sign that these domains are being used by malware. Trying to access the domains via browser, will either get you a landing page or HTTP ERROR 403 (Forbidden). However, we believe that there are server controls that allow access to the malicious extensions based on specific http headers.

All domains are translated to IP addresses belonging to Amazon AWS, part of AS16509. The domains do not share the same IP, and from time to time it seems that the IP for a particular domain is changed dynamically, as can be seen in this example:

tawuhoju.com	13.224.161.119	14/04/2021
tawuhoju.com	13.224.161.119	15/04/2021
tawuhoju.com	13.224.161.22	23/04/2021

tawuhoju.com	13.224.161.22	24/04/2021

Wrapping Up

Given all this evidence, it's clear to us that the infrastructure used on these campaigns is leveraging AWS and that it is a very large campaign. We identified many connection points between 80 C&C domains, identifying their DGA and infrastructure. This could be used to identify the C&C communication and infected machines, by analyzing network traffic. Security teams can now use these insights to identify the traffic from malicious Chrome extensions.

IOC

bacugo[.]com
bagoj[.]com
baguhoh[.]com
bosojojo[.]com
bowocofa[.]com
buduguh[.]com
bujot[.]com
bunafo[.]com
bunupoj[.]com
cagodobo[.]com
cajato[.]com
copamu[.]com
cusupuh[.]com
dafucah[.]com
dagaju[.]com
dapowar[.]com
dubahu[.]com
dubocoso[.]com
dudujutu[.]com
focuquc[.]com
fogow[.]com
fokosul[.]com
fupoj[.]com
fusog[.]com
fuwof[.]com
gapaqaw[.]com
garuq[.]com
gufado[.]com
hamohuhu[.]com
hodafoc[.]com
hoqunuja[.]com
huful[.]com
jagufu[.]com
jurokotu[.]com
juwakaha[.]com
kocunolu[.]com
kogarowa[.]com
kohaguk[.]com
kuqotaj[.]com
kuquc[.]com
lohoqoco[.]com
loruwo[.]com
lufacam[.]com
luhatufa[.]com
mocujo[.]com
moqolan[.]com
muqudu[.]com
naqodur[.]com
nokutu[.]com
nopobuq[.]com
nopuwa[.]com
norugu[.]com

```
nosahof[.]com
nuqudop[.]com
nusojog[.]com
pocakaqu[.]com
ponojuju[.]com
powuwuqa[.]com
pudacasa[.]com
pupahaqo[.]com
qaloqum[.]com
qotun[.]com
qufobuh[.]com
qunadap[.]com
qurajoca[.]com
qusonujo[.]com
rokuq[.]com
ruboja[.]com
sanaju[.]com
sarolosa[.]com
supamajo[.]com
tafasajo[.]com
tawuhoju[.]com
tocopada[.]com
tudoq[.]com
turasawa[.]com
womohu[.]com
wujop[.]com
wunab[.]com
wuqah[.]com
```

References:

[1] https://www.catonetworks.com/blog/threat-intelligence-feeds-and-endpoint-protection-systems-fail-to-detect-24-malicious-chrome-extensions/ [2] https://awakesecurity.com/blog/the-internets-new-arms-dealers-malicious-domain-registrars/

Elad Menahem

Elad Menahem is the Director of Security at Cato Networks. He served in an elite tech unit in the Israel Defense Forces (IDF) Intelligence Corps and has more than 16 years of cybersecurity expertise. Previously, he was an enterprise security research manager at Trusteer, which was acquired by IBM.