Drawing the Line between SYS01 and Ducktail through DNS Traces

Table of Contents

Executive Report

Back in January of this year, we studied the infrastructure of Ducktail, a malware that trailed its sights on Facebook business owners and advertisers. Just this month, Morphisec researchers found a similar threat they've dubbed "SYS01."

While SYS01 bore a striking resemblance to Ducktail at first glance, Morphisec confirmed the two threats weren't one and the same. Using the 10 domains they tagged as indicators of compromise (IoCs) as jump-off points, the WhoisXML API research team sought to make their own comparison, this time focusing on differences between the DNS traces the two malware left. Our analysis found:

- 20 IP addresses to which the domains dubbed as IoCs resolved, two of which turned out to be malicious
- 3,001 domains that shared the IoCs' IP hosts, 21 of which were confirmed to be malware hosts
- Two domains that contained the string ***baglamanotalari.*** akin to one of the IoCs

SYS01 Known Facts

According to the Morphisec study, SYS01, like Ducktail, stole data from Facebook business owners and advertisers and employed the same lures and tactics. What separated SYS01 from Ducktail was its campaign payload—the two malware exhibited different behaviors.

The research listed 10 domains as IoCs, namely:

- caseiden[.]com
- graeslavur[.]com
- rapadtrai[.]com
- baglamanotalari[.]com
- oscarnaija[.]com
- makananwisata[.]com

- seleriti[.]com
- seemlabie[.]top
- craceruib[.]top
- mahinetain[.]top

We sought to trace SYS01's digital footprint to determine if it shared other commonalities with Ducktail apart from its intended targets and the tactics used by its operators.

SYS01 IoC Expansion Analysis

To draw the line between SYS01 and Ducktail, we conducted an IoC expansion analysis for SYS01. That will allow us to identify similar patterns among the two threats' artifacts and web properties, if any.

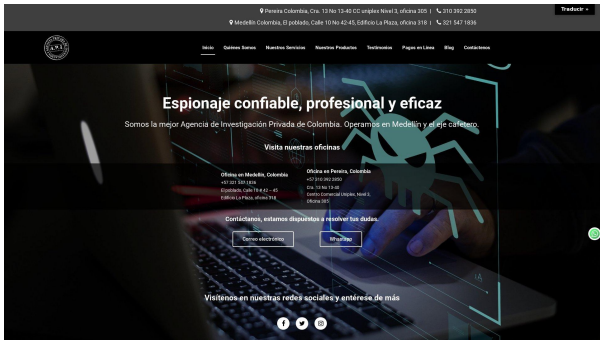
We began with a bulk WHOIS lookup for the IoCs that revealed the following:

- All of the 10 domains were registered via NameSilo, LLC. The Ducktail domains indicated two different registrars.
- The SYS01 IoCs also used a different privacy redaction service—Privacy Guardian.
- All the IoCs were registered in the U.S., the only resemblance we could find with one of the Ducktail IoCs.
- The only similarity we found between the SYS01 and Ducktail domains was that they were all newly registered when they were used in relevant campaigns.

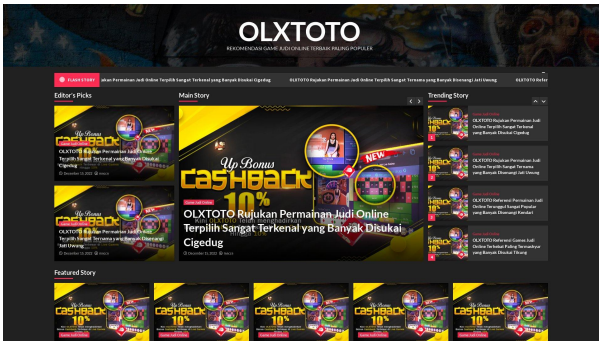
Next, we subjected the SYS01 IoCs to DNS lookups that led to the discovery of 20 unique IP resolutions. SYS01 didn't share any of Ducktail's IP hosts. Also, all the IP addresses were shared hosts and two turned out to be malicious, including 104[.]21[.]43[.]250. They were all geolocated in the U.S., too, again unlike the Ducktail IP host we identified.

To identify other potential SYS01 artifacts, we performed reverse IP lookups that uncovered 3,001 additional domains. None of them were identical to any of the Ducktail IP-connected domains we found earlier. In addition, 21 of them were found to be malicious. Eight of these malware-laden pages continued to host live content, with four of these pages looking suspicious due to reasons detailed along with their screenshots below.

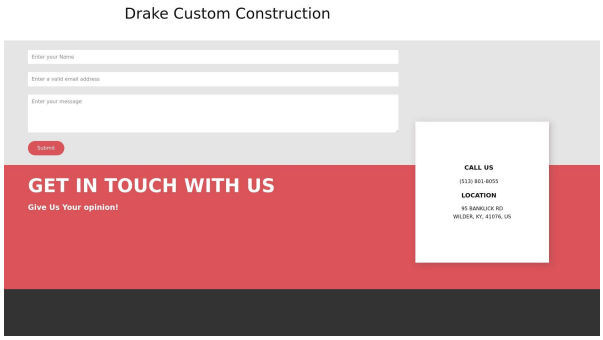
Screenshot of 2021livestream[.]com whose content doesn't match its domain name



Screenshot of detectivesdeleje[.]com that seems to be offering espionage services, which could be considered illegal in many countries



Screenshot of domaljevac[.]net that offers cashback savings, a possible cybercrime lure



Screenshot of drakecustomconstruction[.]com that asks users to give out personally identifiable information (PII), specifically their name and email address, which could be used for phishing

Finally, we looked for domains that shared common strings with the IoCs via Domains & Subdomains Discovery. We found only two that contained the string ***baglamanotalari.***, which only differed from the IoC baglamanotalari[.]com in that it used other top-level domain (TLD) extensions. None of them were found to be malicious. They were also unreachable unlike the IoC that resolved to an error page.

Like all the other SYS01 artifacts we discovered in our analysis, the string-connected domains—baglamanotalari[.]tk and xn--balamanotalar-x2b5z[.]com—didn't share any similarities with the Ducktail ones we identified.

The Bottom Line

Apart from uncovering 3,023 IP addresses and domains that could be part of the SYS01 infrastructure, our IoC expansion analysis also seemingly affirms Morphisec's finding. Despite having the same target and using similar tactics and lures, SYS01 and Ducktail are not one and the same as far as we could tell. They didn't just have varying payloads but also had distinct digital footprints based on the traces they left in the DNS.

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

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 104[.]21[.]63[.]221
- 172[.]67[.]135[.]158
- 104[.]21[.]26[.]75
- 172[.]67[.]192[.]247
- 104[.]21[.]20[.]143
- 172[.]67[.]191[.]191
- 104[.]21[.]43[.]250
- 104[.]21[.]71[.]190
- 172[.]67[.]148[.]21
- 172[.]67[.]168[.]3
- 104[.]21[.]74[.]93

Sample Domains That Shared the IoCs' IP Hosts

- a-great-attorney-tt[.]zone
- a-great-ca-app-developer-course[.]fyi
- a-great-drive-use[.]fyi
- a-great-hoardercleanup[.]fyi
- a-great-in-internet-w-o-landline[.]zone
- a-great-intl-tires[.]fyi
- a-great-latam-audifonos[.]zone
- a-great-us-adhd[.]fyi
- a-great-us-lab-technician-programs[.]fyi
- a-ramirez[.]com
- b[.]kyarsh827[.]workers[.]dev
- b52[.]bio
- b55007[.]com
- b8s[.]xyz
- ba-sw[.]ru[.]com
- baarod[.]com
- babychic507[.]com
- babygoesretros[.]com
- babyretrosale[.]com
- bacjmd[.]xyz
- c1[.]teen-sex[.]me
- c54774[.]com
- c567w[.]com
- c69y0c1u[.]shop
- c718[.]fun
- c7lab[.]com
- ca-onlinedating[.]life
- ca-used-suvs-benefit[.]fyi
- caeridcclhb[.]cyou

- cafewithplug[.]com
- d21[.]one
- d2sonline[.]net
- d37133[.]com
- d67j[.]com
- da3[.]okane[.]my[.]id
- da4[.]okane[.]my[.]id
- daboscarol[.]it
- daconhogafahrmar[.]ga
- daejeon-anma[.]com
- daengstorenih[.]my[.]id
- e-cigarette[.]tech
- e[.]elastisxum[.]online
- e10campus[.]com
- eajwndew[.]work
- eao[.]frbkaleta[.]pl
- earenteslatycomp[.]tk
- earepic[.]com
- earncryptoez[.]com
- earprettercmanvers[.]tk
- easiestchatsforms[.]com
- f4lit[.]shop
- fa[.]shafiei[.]dev
- faces[.]photos
- factline[.]net
- facturacion[.]naturinstant[.]com
- failglamour[.]top
- fairyland-cattery[.]com
- fakehouse[.]tk
- famous-sleep[.]de
- fangtripod[.]com
- gabastio[.]ga
- gabiccemarehotel[.]eu
- gakxithorrio[.]tk
- ganheinosorteio[.]com[.]br
- gastprosadraril[.]ga
- gaymenoldporn[.]com
- gefateslo[.]ga
- genhighta[.]tk
- germananthdarro[.]gq
- gistcompfestnullpefer[.]cf
- guyrenreteli[.]tk
- haberguce[.]com[.]tr
- hahasport[.]fr
- halkias[.]net
- han-fishing[.]com
- hanlathink[.]cf
- hardi-toto[.]com
- harrastajaksi[.]fi
- hatnaudipnea[.]tk
- hcvmt[.]morel-immobilier-dax[.]fr
- 004120[.]com
- 00857cca77b615c369f48ead5f8eb7f3[.]com
- 0123tk[.]com
- 040xx[.]com
- 047rr[.]com
- 081694[.]com
- 08srl[.]homes
- 0dihm1i[.]buzz
- 0djfxp[.]cyou
- 0q8u[.]com
- 1[.]ibnaseed[.]com
- 100at[.]shop
- 100dollarrisk[.]com
- 103l[.]xyz
- 107taste[.]com
- 109876543210[.]nl
- 10ab[.]de
- 10downloader[.]me
- 10joker[.]com
- 10numarashop[.]com

Sample Malicious IP-Connected Domains

- 2021livestream[.]com
- browalvtivenet[.]ga
- chaoticcentury[.]net
- detectivesdeleje[.]com

- domaljevac[.]net
- drakecustomconstruction[.]com
- emilyshoe[.]shop
- 7z84dg[.]cyou
- alishia[.]club
- atlasadolescence[.]cn
- bledkin[.]shop