DNSの痕跡からSYS01とDucktailを明確に区別

目次

要旨

2023年1月、Facebookビジネスアカウントのオーナーや広告主を狙ったマルウェア「Ducktail」のインフラを当社で調査しました。その後2023年4月には、Morphisecの研究者が「SYS01」と呼ばれる同様の脅威を発見しました。

SYS01は一見するとDucktailに似ていますが、Morphisecはこの2つの脅威が同じものでないことを確認しました。そこで、WhoisXMLの研究チームは、Morphisecがセキュリティ侵害インジケーター（IoC）として特定した10個のドメイン名を出発点として、SYS01とDucktailが残したDNSの痕跡の違いに注目し、独自の比較を試みました。その結果、以下を発見しました。

- IoCとされたドメイン名が名前解決した20個のIPアドレス。うち2個には悪意があることを確認
- IoCのIPアドレスを共用していた3,001個のドメイン名。うち21個はマルウェアホストと確認
- IoCの1つと同様に***baglamanotalari***という文字列を含んだ2個のドメイン名

SYS01 – 既知の事実

Morphisecの調査によると、SYS01はDucktailと同様、Facebookビジネスアカウントのオーナーや広告主からデータを盗み、同様のルアーや戦術を採用していました。SYS01がDucktailと異なるのはペイロードであり、2つのマルウェアは異なる挙動を示しました。

Morphisecの調査結果では、以下の10個のドメイン名がSYS01のIoCとして挙げられました。

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

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

当社はこれをもとにSYS01のデジタルフットプリントを追跡し、標的や戦術以外にDucktailとの共通点があるかどうかを調べました。

SYS01のIoCリスト拡張と分析

SYS01とDucktailの違いを見つけるべく、SYS01のIoCリストを拡張する形で調査を広げました。その過程でSYS01とDucktailのアーティファクトとウェブプロパティの中に類似したパターンがあれば特定できると考えたためです。

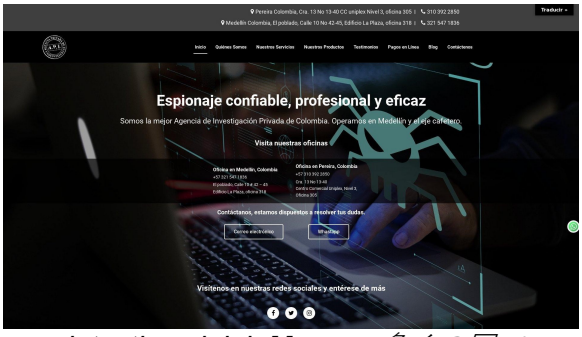
まず、IoCをbulk WHOIS lookupで検索し、以下を発見しました。

- SYS01 IoCの10個のドメイン名は全てNameSilo, LLC経由で登録されたもの。他方、DucktailのドメインIoCは別の2社のレジストラを使用
- SYS01のIoCは、固有のプライバシー保護サービス（Privacy Guardian）を使って登録された
- 全てのIoCは米国で登録されたもの。これは、Ducktail IoCの1つと類似の特徴
- SYS01とDucktailのドメインIoCの唯一の共通点は、悪意あるキャンペーンで使用する時に新規登録されたという点

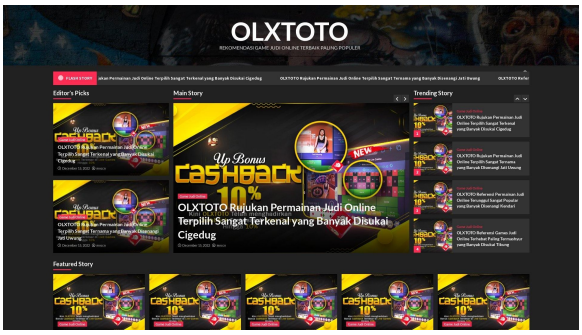
次に、SYS01のIoCをDNS lookupsで検索したところ、20個のユニークなIPアドレスに名前解決しました。SYS01のIoCはDucktail IoCのいずれのIPアドレスも使っていませんでした。また、20個のIPアドレスは全て共用アドレスで、104[.]21[.]43[.]250を含む2つには悪意があることが判明しました。これらのIPアドレスはすべて米国内に位置しており、当社で特定したDucktailのIPアドレスとは異なるものでした。

SYS01のアーティファクトになり得る他のドメイン名を特定するためreverse IP lookupsを使って調べたところ、さらに3,001個のドメイン名が見つかりました。共通のIPアドレスを使っているDucktailのドメインIoCとして当社が特定したものと同じドメイン名は、その中にありませんでした。しかし、21個は悪意あるドメイン名と判明しました。そして、21個のうちの8個は有効なコンテンツをホストし続けており、そのうちの4つのページは疑わしいと判断されました。以下はそれらのページのスクリーンショットです。

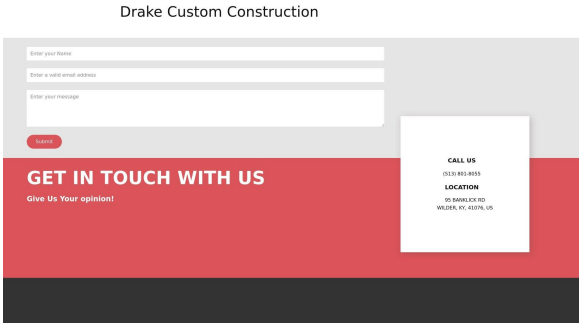
2021livestream[.]com。コンテンツがドメイン名と合致しない



detectivesdeleje[.]com。多くの国で違法とされる諜報サービスを提供しているように見える



domaljevac[.]net。サイバー犯罪のルアーかもしれないキャッシュバック貯蓄を提供している



drakecustomconstruction[.]com。フィッシングに利用されかねない個人情報、特に名前やメールアドレスの提供をユーザーに求めている

最後に、Domains & Subdomains Discoveryを使い、IoCと共通の文字列を持つドメイン名を探しました。その結果、***baglamanotalari***という文字列を含むドメイン名が2つ見つかりましたが、それらはIoCであるbaglamanotalari[.]comとTLDの部分だけが異なり、あとは全く同じ文字列のドメイン名でした。なお、どちらも悪意があるドメイン名ではありませんでした。また、エラーページに行き着くIoCとは異なり、到達不能な状態でした。

今回の分析で発見したSYS01の他のアーティファクトと同様に共通の文字列を含んだドメイン名であるbaglamanotalari[.]tkとxn--balamanotalar-x2b5z[.]comには、当社が見つけたDucktailのアーティファクトとの類似点がありませんでした。

結論

SYS01のインフラの一部となり得る3,023個のIPアドレスとドメイン名を発見したことに加え、当社のIoCリスト拡張分析の結果もまた、Morphisecの発見を裏付ける形となったようです。SYS01とDucktailは同じ標的を狙い似たような戦術やルアーを使っているものの、当社で確認した限り別物です。ペイロードが違うだけでなく、DNSに残された痕跡が示したように、デジタルフットプリントも明確に異なっていました。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

IoCとして特定されたドメイン名が名前解決したIPアドレスの例

- 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

IoCのIPアドレスを共用していたドメイン名の例

- 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

共通のIPアドレスを使用していた悪意あるドメイン名の例

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

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