DNSインテリジェンスでEpsilon Stealerの足跡を辿る

目次

要旨

ゲーマーにとっては自分のコンピューターがEpsilon Stealerに感染したら一巻の終わりですが、危険にさらされているのはゲーマーだけではありません。マルウェアオペレーターに模倣されているEPSILON、Pokemon、Robloxといったゲームのクリエイターもまた、大きな損失を被ることになります。顧客を失い、その過程で評判を落とすかもしれません。

Epsilonは、Discordのメッセージや偽のゲームダウンロードサイトを利用して、ユーザーの認証情報、個人データ、ゲーム内のアセットなどの機密情報を盗み出します。Sekoia.ioのセキュリティ研究者は最近、このデータスティーラーに関する詳細な分析を発表し、その中で133個のドメイン名とサブドメインをセキュリティ侵害インジケーター（IoC）として挙げました。

WhoisXML APIの研究チームはこれを受け、そのIoCリストから76個のドメイン名（以下「ドメインIoC」）を抽出し、それらを足掛かりに膨大なDNSインテリジェンスを駆使して未報告の関連アーティファクトを探しました。その結果、以下を特定することができました：

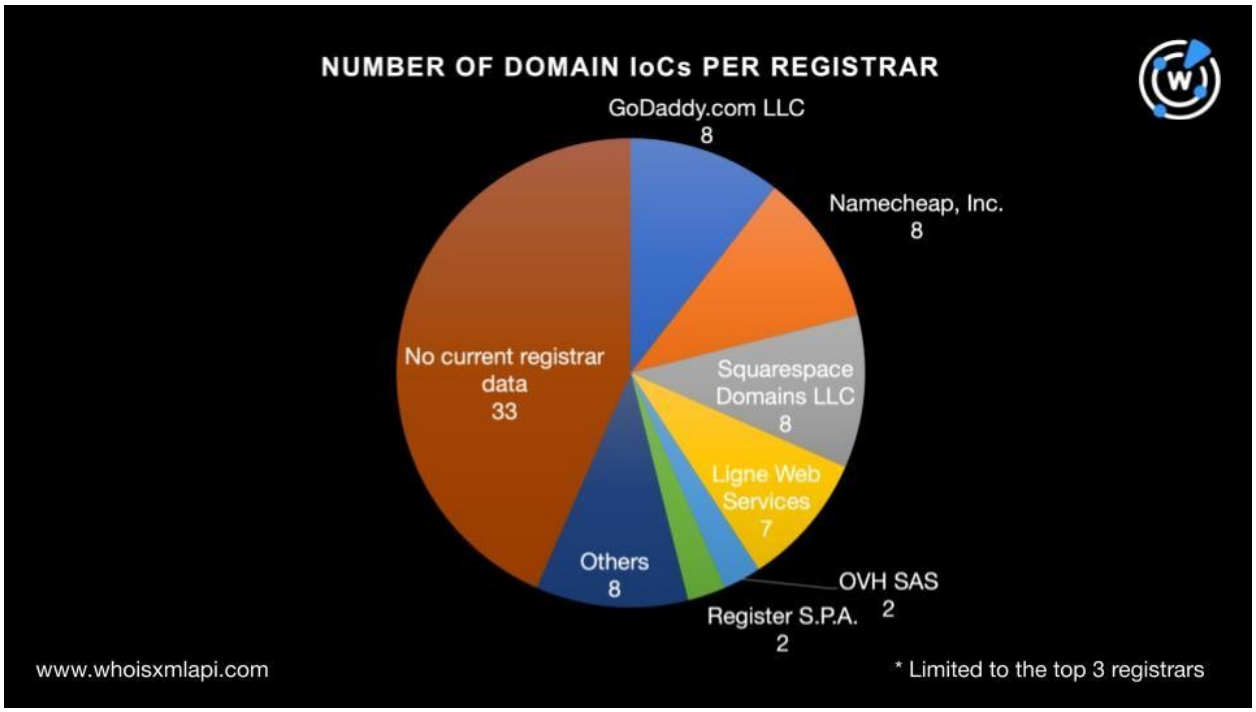
- ドメインIoCと同じメールアドレスを使用していたドメイン名74個
- ドメインIoCが名前解決したIPアドレス33個。そのうち28個は悪意あるIPアドレス
- ドメインIoCと同じ文字列を含むドメイン名1,623個。そのうち2個は悪意あるドメイン名

Epsilon StealerのIoC

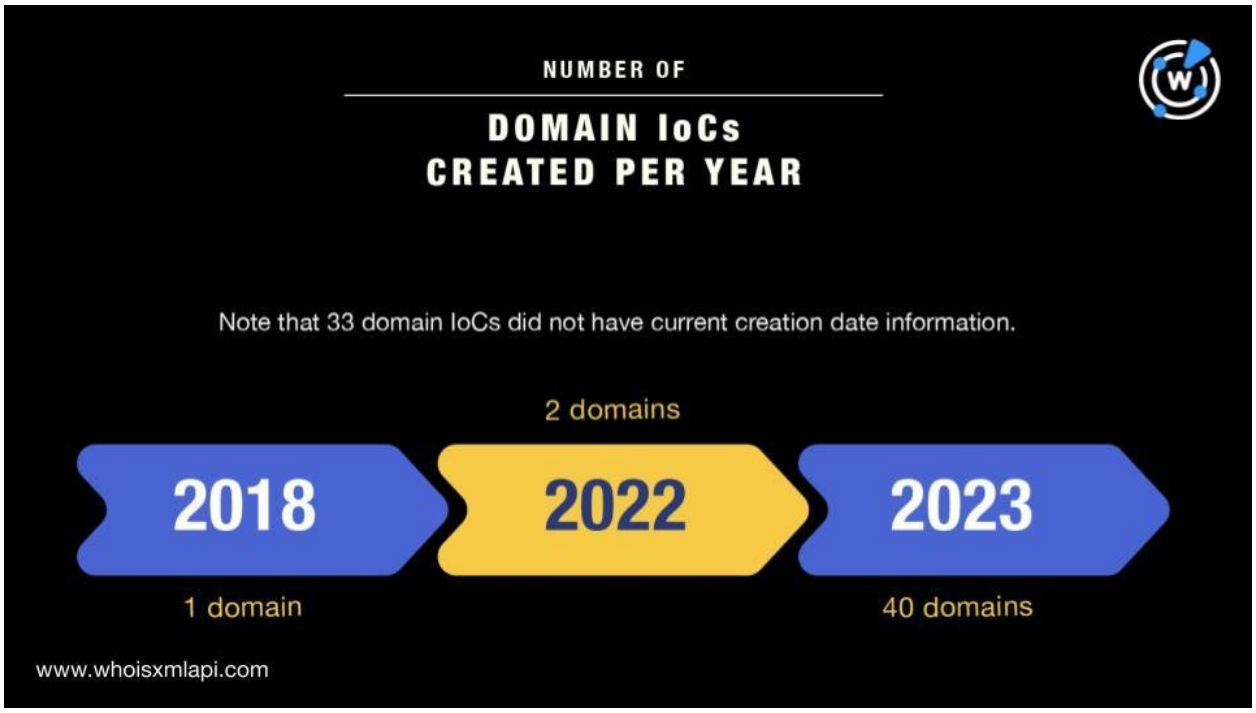
まず、76個のドメインIoCに関する情報を最大限集めるため、それらをBulk WHOIS Lookupで検索しました。その結果、以下のことがわかりました：

- 14社の管理レジストラが特定されました。GoDaddy.com LLC、Namecheap, Inc.、

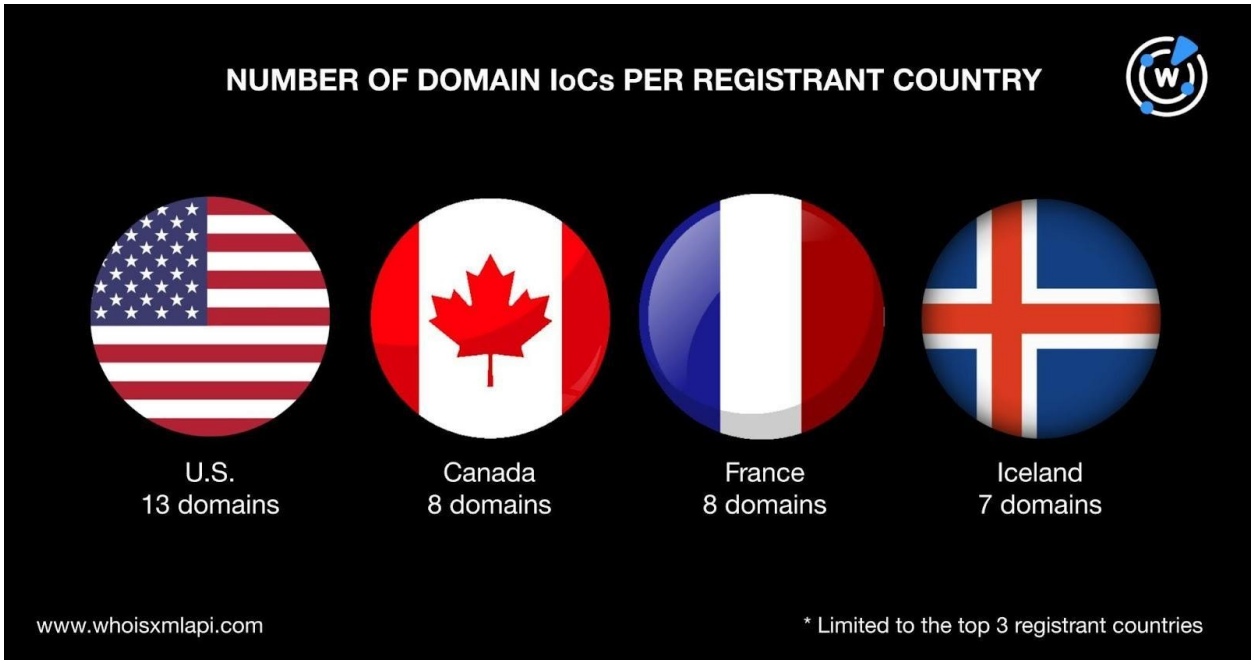
Squarespace Domains LLCがそれぞれ8個、Ligne Web Servicesが7個、OVH SASとRegister S.P.A.がそれぞれ2個を管理しており、別の8社が1個ずつ管理していました。残りの33個のドメインIoCについては、現在のレジストラのデータがありませんでした。



- 43個のドメインIoCは、2018年から2023年の間に新規登録されたものでした。残りの33個は現在のWHOISレコードに登録日の情報が記載されていませんでした。



- ドメインIoCが登録された国のトップ3は、米国（13個）、カナダとフランス（各8個）およびアイスランド（7個）でした。この他、キプロス、オランダ、ルーマニア、トルコで1個ずつ登録されていました。37個は登録者の国の情報がありませんでした。



- plaguehunter[.]comというドメインIoCについては、WHOISで登録者名が公開されていました。

Epsilon StealerのIoCリスト拡張

Epsilon StealerのIoCリストを拡張するべく、ドメインIoC 76個の過去のWHOISレコードを調査しました。

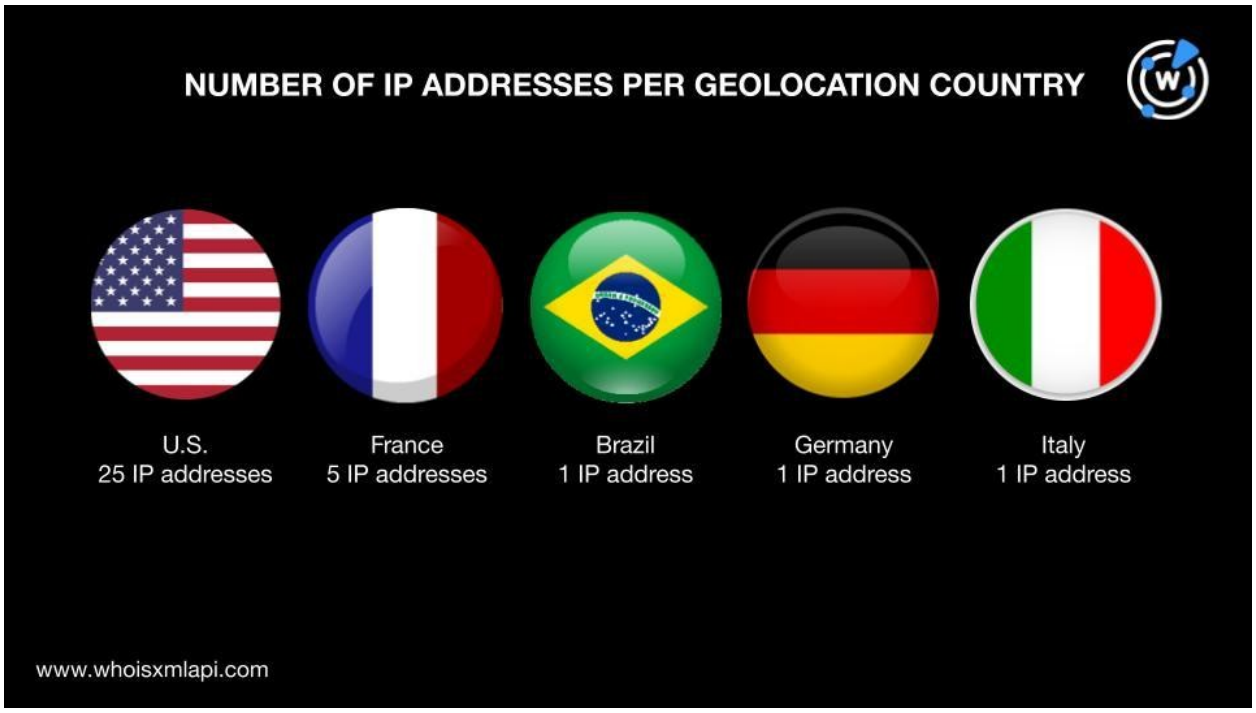
76個をWHOIS History APIで検索した結果、31個の過去レコードに合計32個のメールアドレスが表示されました。また、そのうち9個のメールアドレスは未編集のまま公開されていました。

その9個の公開メールアドレスについてReverse WHOIS APIを実行したところ、重複と既存のドメインIoCを除く74個のドメイン名の現WHOISレコードにも、それらが登録されていました。

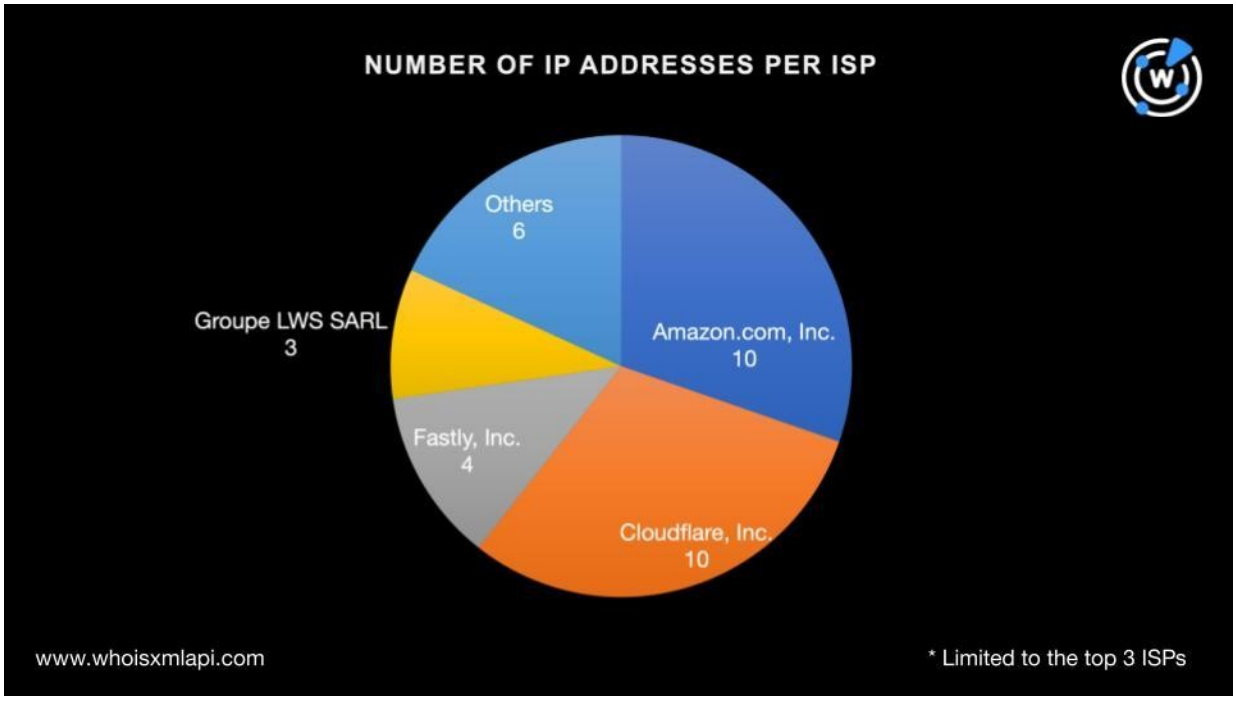
また、DNS Lookupで76個のドメインIoCを検索し重複をフィルタリングした結果、22個のドメインIoCが33個の有効なIPアドレスに名前解決しました。

その33個のIPアドレスをIP Geolocation Lookupにかけた結果から、以下の興味深い事実が明らかになりました：

- 25個は米国を起源とするIPアドレスでした。また、フランスに5個、ブラジル、ドイツ、イタリアに1個ずつ位置していました。



- 33個のIPアドレスの管理ISPとして、10社が特定されました。最も管理アドレス数が多かったのはAmazon.com, Inc.とCloudflare, Inc（各10個）で、次いで多かったのはFastly, Inc.（4個）、Groupe LWS SARL（3個）でした。この他、6社が1個ずつを管理していることがわかりました。



- 33個をThreat Intelligence APIエンジンで調べた結果、28個は悪意あるIPアドレスと判明しました。そのうち5個に関する詳細情報を以下に示します。

IPアドレス	関連する脅威の種類	初見日
104[.]21[.]0[.]216	Generic Malware Phishing	2023年3月29日
104[.]21[.]61[.]207	Malware Suspicious	2023年4月5日
104[.]21[.]63[.]236	Generic Malware Phishing	2023年5月21日
13[.]248[.]169[.]48	C2 Generic Malware Phishing Suspicious	2023年3月28日
13[.]248[.]213[.]45	C2 Generic Malware Phishing Suspicious	2023年12月7日

最後に、Domains & Subdomains Discoveryを使い、ドメインIoCに含まれている48種類のテキスト文字列（以下）のいずれかを同様に含んでいる他のドメイン名を探しました：

- **abyssgame**
- **aqua-phobia**
- **aquafridge**
- **articpunk**
- **conditus**
- **conquistadorio**
- **creseller**
- **deadlegacy**
- **deadsould**
- **dualcorps**
- **epsilon1337**
- **fightordie**
- **flstudiocrack**
- **grimwalker**
- **hentaimaster**
- **homurahime**
- **inovaperf**
- **legacysurvival**
- **movesoul**
- **mythicguardian**

- nobodysleft
- plaguehunter
- pokemonadventure
- pokemonaventure
- rolaslegacy
- ronawind
- samuraihime
- shirokim
- shirone
- siltgame
- siltproject
- slayercat
- snotragame
- spacewars-beta
- spiralcircusgame
- strangerlegends
- survival-machine
- theblacktail
- timberstory
- trailofnanook
- ultra-flighter
- unturned
- vaniapunk
- voidofspace
- voidvanguard
- wdb.
- weavergames
- worldofsymphony

その結果、1,623個のドメイン名が検出されました。それらに対してThreat Intelligence APIを実行したところ、2個は悪意あるドメイン名でした。以下はその詳細です。

ドメインIoCと同じ文字列を含むドメイン名	関連する脅威の種類	初見日
dualcorps[.]site	Generic	2023年11月2日
unturnedplayable[.]com	Phishing	2023年3月9日

—

Epsilon Stealerについて行った今回の調査で、潜在的関連アーティファクト（悪意あるIPアドレス28個およびIoCと同じ文字列を持つ悪意あるドメイン名2個を含む）が合計1,730個検出されました。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IoCと同じメールアドレスを使用していたドメイン名の例

- 4006118263[.]xyz
- 4805058877[.]xyz
- adslw[.]xyz
- aisoge[.]xyz
- aisouge[.]xyz
- azcy[.]xyz
- azfc[.]xyz
- azgw[.]xyz
- azjr[.]xyz
- azlc[.]xyz
- azlx[.]xyz
- azly[.]xyz
- ben-simmons[.]xyz
- breakthroughenergycoalition[.]xyz
- cangbi[.]xyz
- demonoton[.]com
- detedium[.]com
- dianguan[.]xyz
- emoticombat[.]com
- haodaizhi[.]xyz

IoCが名前解決したIPアドレスの例

- 104[.]21[.]0[.]216
- 104[.]21[.]48[.]205
- 104[.]21[.]51[.]98
- 104[.]21[.]61[.]207
- 104[.]21[.]63[.]236
- 13[.]248[.]169[.]48
- 13[.]248[.]213[.]45
- 15[.]197[.]142[.]173
- 172[.]67[.]128[.]80
- 172[.]67[.]156[.]47
- 172[.]67[.]173[.]25
- 172[.]67[.]178[.]135
- 172[.]67[.]214[.]140
- 18[.]213[.]222[.]111
- 185[.]135[.]132[.]50
- 185[.]199[.]108[.]153
- 185[.]199[.]109[.]153
- 185[.]199[.]110[.]153
- 185[.]199[.]111[.]153
- 185[.]98[.]131[.]192

IoCと同じ文字列を含むドメイン名の例

- abyssgame[.]club
- abyssgame[.]com
- abyssgame[.]ws
- abyssgamecenter[.]com
- abyssgamecenter[.]ph
- abyssgamer[.]com
- abyssgamers[.]com
- abyssgamers[.]com[.]br
- abyssgamers[.]teaml
- abyssgamerx[.]com
- abyssgames[.]ca
- abyssgames[.]com
- abyssgames[.]de
- abyssgames[.]io
- abyssgames[.]net
- abyssgames[.]tk
- abyssgamestore[.]com
- abyssgameworks[.]com
- aqua-phobia1st[.]co[.]uk
- aqua-phobia1st[.]com
- aquafridge[.]com
- aquafridge[.]info

- aquafridge[.]net
- aquafridge[.]org
- articpunk[.]games
- articpunk[.]xyz
- conditus[.]at
- conditus[.]be
- conditus[.]co[.]uk
- conditus[.]com
- conditus[.]com[.]au
- conditus[.]com[.]mx
- conditus[.]group
- conditus[.]info
- conditus[.]it
- conditus[.]lt
- conditus[.]net
- conditus[.]nl
- conditus[.]org
- conditus[.]se
- conditus[.]si
- conditus[.]tech
- conditus[.]vg
- condituscapital[.]com
- condituscatering[.]co[.]uk
- condituscoulis[.]com
- conditusfitness[.]com
- conditusspices[.]com
- conquistadorio[.]info
- conquistadorio[.]xyz
- creseller[.]com
- creseller[.]xyz
- cresellerhosting[.]com
- cresellers[.]com
- cresellersresource[.]com
- deadlegacy[.]cn
- deadlegacy[.]co
- deadlegacy[.]co[.]uk
- deadlegacy[.]com
- deadlegacy[.]net
- deadlegacy[.]online
- deadlegacy[.]ru
- deadlegacy[.]se
- deadlegacy[.]site
- deadlegacy[.]store
- deadlegacye-sports[.]com
- deadlegacymx[.]com
- deadlegacyreviews[.]com
- deadlegacyusa[.]com
- deadsouldesigns[.]com
- dualcorps[.]com
- dualcorps[.]online
- dualcorps[.]site
- dualcorps[.]xyz
- dualcorpsactivities[.]com
- epsilon1337[.]xyz
- fightordie[.]cf
- fightordie[.]club
- fightordie[.]co
- fightordie[.]co[.]uk
- fightordie[.]com
- fightordie[.]com[.]au
- fightordie[.]com[.]br
- fightordie[.]de
- fightordie[.]eu
- fightordie[.]ga
- fightordie[.]info
- fightordie[.]it
- fightordie[.]ml
- fightordie[.]net
- fightordie[.]org
- fightordie[.]pl
- fightordie[.]ru
- fightordie[.]tk
- fightordie[.]us
- fightordieapparel[.]com
- fightordieclothing[.]com
- fightordiee[.]us
- fightordiemovie[.]com