

DarkTortilla の他の脅威ベクターを発見

目次

1. [要旨](#)
2. [付録：アーティファクトと IoC のサンプル](#)

要旨

DarkTortilla が示すように、古くからデジタルの世界に脅威として存在するフィッシングは、時代とともに巧妙化し続けています。Cyble Research and Intelligence Labs (CRIL) は、Cisco と Grammarly を標的とした脅威の[技術分析](#)を発表しています。果たして、潜在的な脅威のベクトルは他にもあるのでしょうか？

WhoisXML API では、3つの IoC（セキュリティ侵害インジケター）をもとに、調査を水平展開する形で行いました。その結果、以下がわかりました。

- ドメイン名が2個の IP アドレスに名前解決
- 300件を超えるドメイン名が IoC と同じ IP アドレスを使用、そのうち2件は悪意のドメイン名と判明
- 11,358件あまりのドメイン名が Cisco、Grammarly または Atommm という文字列を含み、他の不正行為に使用されている可能性がある。それらのうち正規の企業に属しているらしいものはわずか4%。23件のドメイン名が悪意あるものと確認された。

DNS の繋がり

CRIL のレポートでは、cicsom[.]com と gnammarly[.]com という2件のドメイン名および [https://atommm\[.\]com\[.\]br/\[.\]well-known/acme-challenge/olFjawtld\[.\]png](https://atommm[.]com[.]br/[.]well-known/acme-challenge/olFjawtld[.]png) という URL を IoC としています。

それらを [DNS lookups](#) で検索したところ、104[.]21[.]15[.]248 および 172[.]67[.]165[.]88 という2つの IP アドレスを発見しました。いずれの IP アドレスも地理的な所在は米国で、Cloudflare, Inc.が管理しているものでした。

また、[Reverse IP lookups](#) で調べた結果、関連している可能性のあるドメイン名が少なくとも300件見つかりました。そうしたドメイン名を一括マルウェアチェックにかけたところ、bridgesconstructionsservicesinc[.]com と cl7q5s[.]cyou は悪意あるドメイン名であることがわかりました。

Bridges Construction Services

Enter your Name

Enter a valid email address

Enter your message

Submit

GET IN TOUCH WITH US

Give Us Your opinion!

CALL US
(510) 760-4725

LOCATION
2112 PLACER DR.
SAN LEANDRO, CA 94578

bridgesconstructionservicesinc[.]com のスクリーンショット

WHOIS との関連

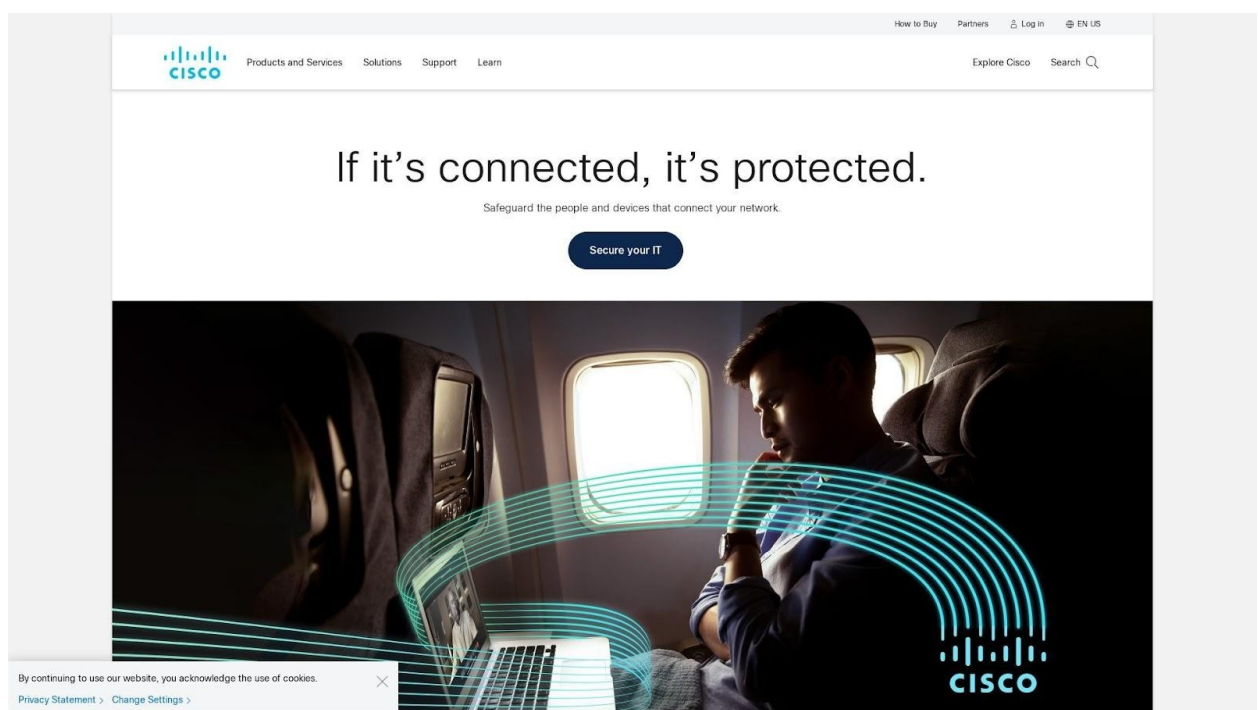
このフィッシング詐欺師は正規の企業を標的にしていたため、当社ではサイバースクワッティングの可能性がある他のドメイン名を探しました。[Domains & Subdomains Discovery](#)で Cisco、Grammarly および Atommm を検索語としつつ、IoC に類似したドメイン名を探すことに注力しました。

その結果、少なくとも 11,358 件のドメイン名が見つかり、うち 23 件は悪意のドメイン名と判明しました。悪意のドメイン名のうち 21 件はマルウェアのホスト、1 つはスパムのホストとして、もう 1 つはフィッシングのページに使用されていることが確認されました。悪意あるドメイン名のうち 10 件を以下に紹介します。

悪意あるドメイン名	カテゴリー
cisco[.]work	マルウェア
cisco[.]asia	マルウェア
cisco[.]pics	マルウェア
ciscoprop[.]ru	マルウェア
shopcisco[.]eu	マルウェア

ciscoav[.]com	フィッシング
grammarly[.]pics	マルウェア
grammarlyget[.]com	マルウェア
appgrammarly[.]info	マルウェア
mygrammarly[.]co	スパム

悪意あるドメイン名の中には、企業のブランド名のタイポスクワッティングで使われているものに加え、企業の正規のページにリダイレクトするものもあるようでした。[screenshot lookup](#)で見つけた例を以下に示します。



cisco[.]com にリダイレクトする cisco[.]pics

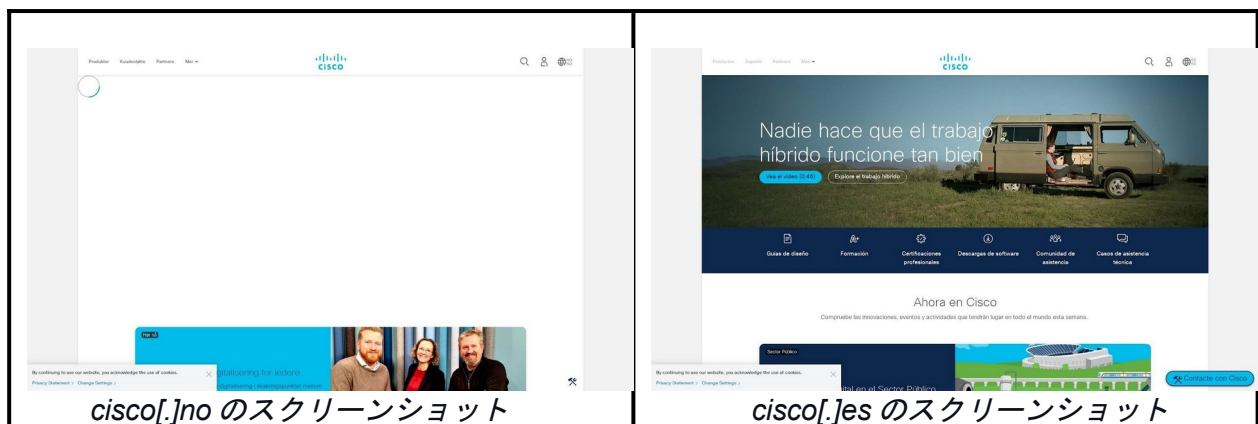
次に、11,000 件を超える潜在的なサイバースクワッティングドメイン名の WHOIS レコードを、正規の企業ドメイン名のレコードと比較しました。その結果、模倣された正規の組織が所有するドメイン名はわずか 451 件にすぎないとわかりました。Cisco は WHOIS レコードを非公開にしていなかったため、比較は容易にできました。他方、WHOIS レコードの一部を非公開にしていた Grammarly の場合、比較はそれほど簡単ではありませんでした。

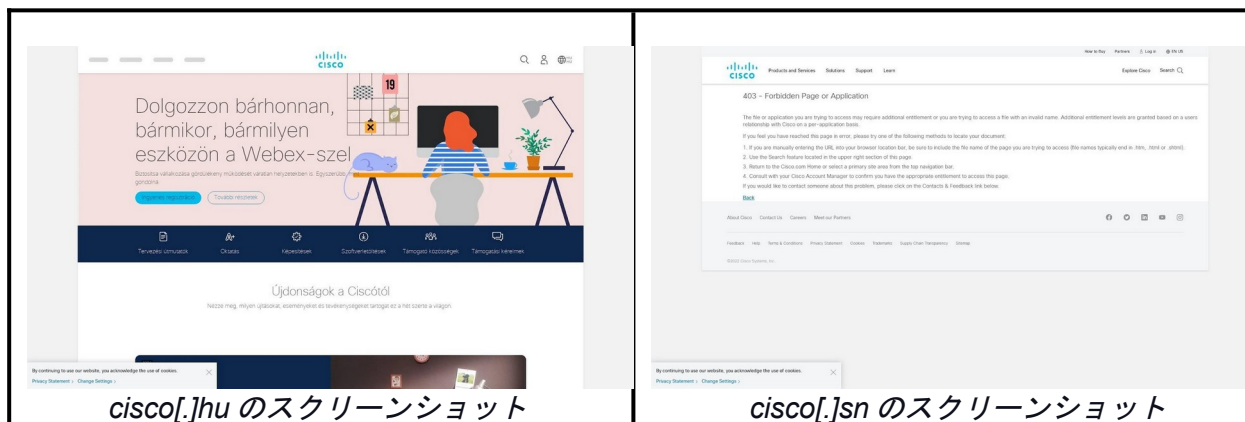
Grammarly に見た目が似ているドメイン名は、二段階の方法で抽出する必要がありました。まず Domains By Proxy, LLC 以外のレジストラを使っているドメイン名を除外しました。次に、レジストラ名が GoDaddy.com, LLC 以外になっているドメイン名を取り除きました。その結果、Grammarly のブランド名を含む 476 件のドメイン名のうち、Grammarly が所有していると思われるドメイン名はわずか 27 件とわかりました。

下の表は、ドメイン名の所有を判断するために我々が使用した WHOIS の情報を示しています。

企業名	正規のドメイン名	比較パラメーターとして 使用された WHOIS データ
Cisco	cisco[.]com	Administrative email address: infosec@cisco[.]com
Grammarly	grammarly[.]com	Registrant organization: Domains By Proxy, LLC Registrar name: GoDaddy.com, LLC

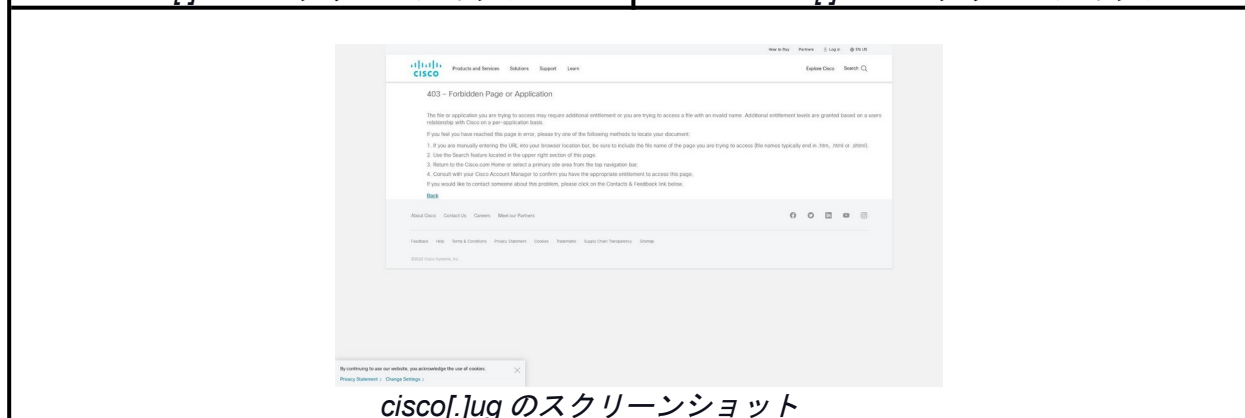
また、他のページにリダイレクトされないと仮定し、フィッシングページや他のマルウェアの配布元となりうる、見た目の似たドメイン名のスクリーンショットも入手しました。Cisco と Grammarly の調査で使用したものは WHOIS レコードの情報が異なる、疑わしいウェブページの例を以下に示します。





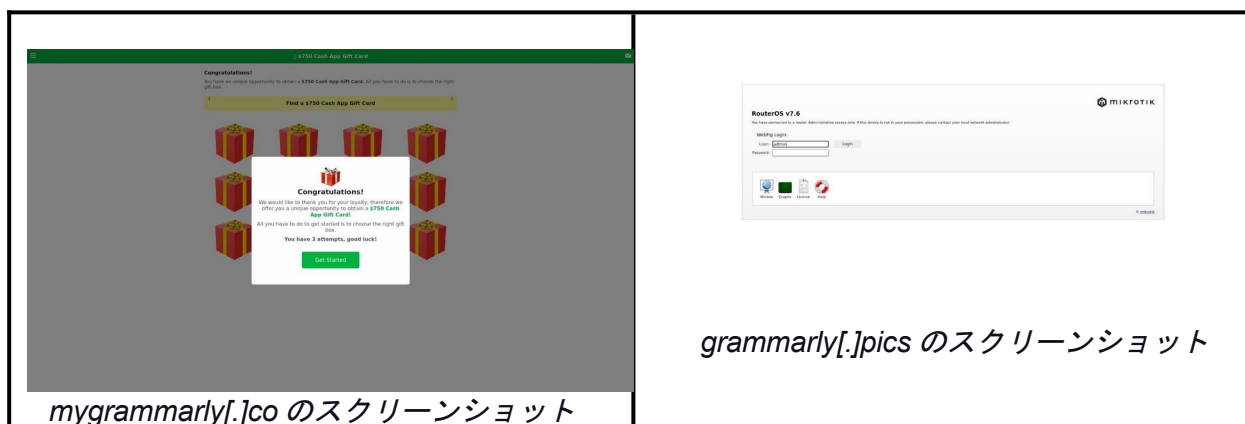
cisco[.]jhu のスクリーンショット

cisco[.]sn のスクリーンショット



cisco[.]jug のスクリーンショット

見た目の似たドメイン名のウェブページには、なりすましている企業のロゴやコンテンツが掲載されていないものもあります。とはいえ、それらはいとも簡単に個人情報を入力させ、訪問者をフィッシングや詐欺に遭わせる危険があります。以下に、ゲームをすると賞品が当たるページやログインのページをホストしている不審なドメイン名の例を示します。



mygrammarly[.]co のスクリーンショット

grammarly[.]pics のスクリーンショット

今回、IP アドレス、DNS、WHOIS のデータを活用して IoC の調査を横展開した結果、DarkTortilla と関連している可能性のあるアーティファクトを 11,600 余り発見できました。また、Cisco や Grammarly の顧客をスパム、フィッシング、マルウェア感染の危険にさらす可能性のある悪意のドメイン名を 29 件特定できました。

同様の調査をご希望のお客様、またはこの調査の全データ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 のサンプル

CRIL と AlienVault で確認された IoC

- cicsom[.]com
- atomm[.]com[.]br
- gnammarly[.]com

IoC と確認されたドメイン名が名前解決した IP アドレス

- 104[.]21[.]15[.]248
- 172[.]67[.]165[.]88

一部の IoC と同じ IP アドレスを使っていたドメイン名のサンプル

- a5t18ra2[.]top
- abchisilotyrel[.]tk
- abraajaula[.]com
- acaiteria19k[.]pwa[.]app[.]br
- acheizap[.]pwa[.]app[.]br
- acostafam[.]net
- admin[.]jjonosheba[.]planetxinc[.]xyz
- adriaticreal[.]cz
- adtiojor[.]tk
- africanad[.]ca
- agencies[.]ticketyboo[.]cloud
- aple-pigina[.]vip
- ai[.]jaymcgrath[.]id[.]au
- aircylindertubes[.]today
- ajfheijdfj[.]cf
- akeyplan[.]com
- akgplb[.]com
- alaltalitalsma[.]tk
- alexandresa[.]com[.]br
- alhermayrmouncee[.]ml
- allrushprint[.]com
- allstar-ab[.]org
- almisrotheble[.]tk
- alphanetworks[.]com[.]sg
- altapharma[.]com[.]ua
- amazondiscount[.]walmartpayout[.]com
- amazonpaypal[.]walmartpayout[.]com
- amazonsale[.]walmartpayout[.]com
- amazonshop[.]walmartpayout[.]com
- amazonstore[.]walmartpayout[.]com
- amenta[.]ml
- amolcalsoca[.]gq
- amomitjare[.]ml
- amticarfuzz[.]tk
- anaxnisbatuna[.]gq
- andersklettern[.]de
- androidapksdl[.]com
- animalprotectors[.]us

- ankecata[.]gq
- annecaconkovspe[.]cf
- anru[.]dk
- antarestecnologia[.]com[.]br
- anygoods[.]be
- api[.]jonosheba[.]planetxinc[.]xyz
- api[.]shebok[.]planetxinc[.]xyz
- app[.]mitch[.]guru
- app[.]ticketyboo[.]cloud
- ar9qpb[.]shop
- aralclubanprat[.]ml
- archeologleszno[.]com

一部の IoC と同じ IP アドレスを使っていた悪意のドメイン名

- bridgesconstructionservicesinc[.]com
- cl7q5s[.]cyou

Cisco、Grammarly、Atommm を含むドメイン名の例

- cisco[.]tv
- cisco[.]no
- cisco[.]tn
- cisco[.]ci
- cisco[.]jp
- cisco[.]es
- cisco[.]hu
- cisco[.]sn
- cisco[.]kr
- cisco[.]yt
- cisco[.]id
- cisco[.]ir
- cisco[.]bs
- cisco[.]ug
- cisco[.]uz
- cisco[.]mw
- cisco[.]us
- cisco[.]lv
- cisco[.]mp
- cisco[.]nf
- cisco[.]gg
- cisco[.]io
- cisco[.]so
- cisco[.]xn--ses554g
- cisco[.]la
- cisco[.]rs
- cisco[.]xn--xhq521b
- cisco[.]at
- cisco[.]fm
- cisco[.]im
- cisco[.]ng
- cisco[.]co
- cisco[.]gr
- cisco[.]vc
- cisco[.]se
- cisco[.]cl
- cisco[.]uk
- cisco[.]pe
- cisco[.]kg
- cisco[.]sc
- cisco[.]ro
- cisco[.]cg
- cisco[.]xn--3ds443g
- cisco[.]xn--rhqv96g
- cisco[.]dk
- cisco[.]in
- cisco[.]je
- cisco[.]su
- cisco[.]lk
- cisco[.]ee
- cisco[.]kn
- cisco[.]sh

- cisco[.]pn
- cisco[.]ag
- cisco[.]eu
- cisco[.]bi
- cisco[.]nu
- cisco[.]de
- cisco[.]re
- cisco[.]cc
- cisco[.]xn--io0a7i
- cisco[.]pk
- cisco[.]gy
- cisco[.]al
- cisco[.]xn--vuq861b
- cisco[.]xn--55qx5d
- cisco[.]ws
- cisco[.]is
- cisco[.]ie
- cisco[.]tw
- cisco[.]am
- cisco[.]si
- cisco[.]bz
- cisco[.]sg
- my[.]cisco
- ciscobusiness[.]cisco
- cisco[.]mx
- cisco[.]gl
- cisco[.]fi
- cisco[.]hk
- cisco[.]ba
- cisco[.]ru
- cisco[.]lt
- cisco[.]az
- cisco[.]ae
- cisco[.]mk
- cisco[.]to
- cisco[.]tt
- cisco[.]pm
- cisco[.]tm
- cisco[.]by
- cisco[.]ge
- cisco[.]ml
- cisco[.]me
- cisco[.]ch
- cisco[.]cz
- cisco[.]fr
- cisco[.]lu
- cisco[.]vn
- cisco[.]sv
- cisco[.]it
- cisco[.]cm
- cisco[.]vu
- cisco[.]mn
- cisco[.]be
- cisco[.]cn
- cisco[.]eg
- cisco[.]kz
- cisco[.]pw
- cisco[.]rw
- cisco[.]my
- cisco[.]sk
- cisco[.]pt
- cisco[.]ca
- cisco[.]ua
- cisco[.]mo
- cisco[.]hm
- cisco[.]vg
- cisco[.]ma
- cisco[.]pl
- cisco[.]bg
- cisco[.]hr
- cisco[.]nl
- cisco[.]xn--fiqs8s
- cisco[.]pr
- cisco[.]gm
- cisco[.]li
- cisco[.]dev
- cisco[.]xn--q9jyb4c
- cisco[.]pro
- xcisco[.]es
- cisco[.]xn--6qq986b3xl

- cisco[.]se
- scisco[.]it
- cisco[.]soy
- cisco[.]icu
- cisco[.]cn
- ciscoo[.]be
- ciscos[.]fr
- cisco[.]it
- cisco[.]ro
- xn--cisco-lza[.]com
- ciscoo[.]us
- cisco[.]de
- ciscos[.]pw
- ciscoo[.]cn
- cisco1[.]tk
- ciscos[.]cn
- vcisco[.]de
- ciscos[.]eu
- cisco[.]one
- ciscod[.]vg
- cisco[.]pk
- cisco[.]com
- cisco[.]bid
- scisco[.]se
- ciscos[.]us
- cisco[.]eu
- xcisco[.]ru
- scisco[.]de
- cisco[.]jo
- cisco[.]how
- nic[.]cisco
- ciscox[.]ru
- cisco5[.]ph
- acisco[.]ru
- scisco[.]cn
- wcisco[.]us
- acisco[.]uk
- ciscoo[.]co
- ciscoc[.]ru
- cisco[.]biz
- ccisco[.]cn
- cisco3[.]ml
- cisco[.]ch
- xn--cisco-vw5a[.]com
- ncisco[.]es
- cisco[.]xxx
- cisco[.]co
- ecisco[.]ro
- cisco0[.]tk
- 2cisco[.]ru
- xn--cisco-vpa[.]com
- cisco[.]de
- cisco[.]org
- xn--cisco-rxb[.]com
- zcisco[.]cn
- cisco[.]in
- cisco2[.]tk
- ycisco[.]cn
- ciscoo[.]ir
- cisco[.]mom
- xn--cisco-5pa[.]com
- cisco[.]gd
- cisco[.]fr
- ecisco[.]de
- 4cisco[.]ru
- tcisco[.]ru
- acisco[.]ml
- scisco[.]nl
- cisco[.]be
- xn--cisco-qp[.]com
- io[.]cisco
- scisco[.]ca
- cisco[.]ir
- ciscoo[.]ml
- scisco[.]co
- cisco[.]cn
- cisco[.]de
- cisco[.]oo
- cisco[.]xin
- cisco[.]cf

- cisco[.]moe
- ciscoo[.]eu
- xn--cisc-ogb[.]com
- cisco[.]rip
- ciscoc[.]ph
- ncisco[.]mx
- icisco[.]cn
- ciscoo[.]in
- ciscos[.]fm
- cisco[.]pub
- cisco[.]bar
- ciscoa[.]tk
- cisco3[.]tk
- ciscociscoparty[.]party
- cisco3[.]cf
- ciscom[.]uk
- cisco[.]nyc
- ecisco[.]ir
- cisco[.]lol
- cisco5[.]cn
- scisco[.]fr
- aci[.]cisco
- scisco[.]in
- cisco[.]cat
- ciscoh[.]co
- cisco[.]ceo
- ciscom[.]fi
- ciscom[.]dk
- lcisco[.]ru
- ciscom[.]eu
- icisco[.]ru
- ciscom[.]us
- ciscom[.]tk
- ciscon[.]ru
- ciscog[.]ph
- ciscom[.]nl
- cisco[.]onl
- scisco[.]jp
- cisco[.]lu
- cisco[.]krd
- 1cisco[.]cn
- cisco[.]red
- ciscom[.]fr
- cisco5[.]cf
- icisco[.]ir
- 4cisco[.]es
- cisco2[.]tw
- ciscom[.]ru
- xn--cisc-jra[.]com
- cisco[.]top
- cisco[.]fit
- ciscon[.]nl
- ciscon[.]nu
- acisco[.]tk
- ciscoi[.]cf
- icisco[.]cc
- cisco[.]llc
- 4cisco[.]be
- ciscoa[.]co
- cisco[.]cfd
- cisco[.]ink
- ciscox[.]io
- cisco1[.]ru
- ciscon[.]ca
- scisco[.]nu
- ncisco[.]de
- cisco[.]bot
- cisco[.]ovh
- ciscop[.]co
- ciscom[.]co
- scisco[.]me
- ciscom[.]ie
- wcisco[.]cn
- cisco[.]ist
- cisco[.]kim
- cisco[.]app
- cisco[.]edu
- ciscom[.]in
- cisco[.]fun
- xcisco[.]cn

- cisco[.]cam
- ciscos[.]co
- cisco1[.]ir
- cisco[.]cc
- cisco[.]tel
- ciscod[.]it
- icisco[.]us
- ciscoo[.]tk
- atomm[.]net
- atomms[.]org
- atommortgages[.]com
- atommastering[.]com
- atommerchant[.]com
- atommodels[.]me
- atommooremacro[.]net
- atommotorcompany[.]com
- atommogul[.]com
- atomme[.]club
- atommieoilese[.]com
- atommarkets[.]com[.]vn
- atommoser[.]ch
- atommuelluntermbundestaglagern[.]de
- atommrs[.]com
- atommarla[.]top
- atommuseum[.]de
- atomminerals[.]com[.]au
- atommashines[.]website
- atommuhendisi[.]com
- atommuell[.]com
- atommakers[.]com
- atommaticapplianceservice[.]com
- atomma[.]uk
- atommic[.]xyz
- atommoto[.]com
- atommyco[.]com
- atommatter[.]se
- atommedia[.]me
- atommuzeum[.]cz
- atomminerals[.]com
- atommix[.]com
- atommolecules[.]com
- atommedia[.]co[.]bw
- atommedia[.]studio
- atommatter[.]org
- atommusic[.]net
- atommix[.]site
- atommediastudios[.]com
- atommickbrane[.]com
- atommodelleri[.]xyz
- atommhu[.]tk
- atommultiexpres[.]com
- atommix[.]pl
- atommodelleri[.]com
- atommeeting[.]com
- atommodulars[.]org
- atommfitness[.]com
- atommilano[.]com
- atommobile[.]mobi
- atomm-and-company[.]jp
- atommc[.]net
- atommy[.]network
- atommodell[.]de
- atommy[.]online
- atommy[.]ru
- atommobilty[.]com
- atommovies[.]com
- xn--atommlreport-0ob[.]de
- atommc[.]nl
- atomms[.]com
- atommark[.]com
- atommidia[.]com[.]br
- atommars[.]com
- atommatter[.]es
- atommap[.]org
- atommail[.]us
- atommanager[.]com
- atommorgan[.]com
- atomm[.]com
- atommuell[.]info

- atommalul[.]com
- atommanagement[.]com
- atommodule[.]com
- atommarkt[.]net
- atommodular[.]net
- atommachines[.]net
- atommica[.]org
- atommed[.]ltd
- atomminds[.]com
- atommonitor[.]pl
- atommarkets[.]vn
- atommarketsvn[.]com
- atommawan[.]tk
- atommobile[.]id
- atommehmetdeniz[.]com
- atommobileshop[.]com
- atommovies[.]xyz
- atomm3d[.]com
- atommetin2[.]org
- atommonga[.]art
- atomming[.]com
- atommp3[.]com
- atommedicalegypt[.]com
- atommailbox[.]com
- atommoty[.]website
- atommodern[.]makeup
- atomman[.]ru
- atommlearning[.]co[.]uk
- atommedya[.]com
- grammarlygrammarly[.]com
- grammarly[.]it
- grammarly[.]eu
- grammarly[.]ai
- grammarly[.]xn--mxtq1m
- grammarly[.]io
- grammarly[.]lv
- grammarly[.]tw
- grammarly[.]de
- grammarly[.]au
- grammarly[.]ch
- grammarly[.]gq
- grammarly[.]sg
- grammarly[.]dk
- grammarly[.]fr
- grammarly[.]in
- grammarly[.]ca
- grammarly[.]ga
- grammarly[.]uz
- grammarly[.]at
- grammarly[.]pt
- grammarly[.]xn--kprw13d
- grammarly[.]nz
- grammarly[.]sk
- grammarly[.]co
- grammarly[.]pw
- grammarly[.]hk
- grammarly[.]cn
- grammarly[.]uk
- grammarly[.]ws
- grammarly[.]no
- grammarly[.]us
- grammarly[.]ru
- grammarly[.]kr
- grammarly[.]vg
- grammarly[.]xn--kpry57d
- grammarly[.]ml
- grammarly[.]be
- grammarly[.]xn--fiqs8s
- grammarly[.]jp
- grammarly[.]cm
- grammarly[.]cz
- grammarly[.]nl
- grammarly[.]se
- grammarly[.]xn--fiqz9s
- grammarly[.]cf
- grammarly[.]vn
- grammarly[.]xn--node
- grammarly[.]app
- grammarly[.]xin
- grammarlys[.]cn

- grammarly[.]mom
- grammarly[.]net
- grammarly[.]org
- grammarly[.]top
- grammarly[.]icu
- grammarly[.]gdn
- grammarly[.]ltd
- xn--grammrly-dza[.]com
- grammarly[.]new
- grammarly[.]xyz
- grammarly[.]one
- xn--grammrly-3ya[.]com
- grammarly[.]ink
- xn--grmmarly-9ya[.]com
- grammarly[.]run
- grammarly[.]pro
- grammarly[.]com
- grammarly[.]vip
- igrammarly[.]cn
- grammarly[.]dev
- grammarly[.]xn--ngbrx
- grammarly[.]cam
- grammarly[.]biz
- grammarlycz[.]cz
- grammarlys[.]net
- grammarly[.]tech
- grammarly[.]wang
- grammarly[.]mobi
- mgrammarly[.]com
- grammarly7[.]com
- mygrammarly[.]co
- grammarly[.]club
- grammarly[.]plus
- grammarlys[.]one
- ggrammarly[.]com
- fgrammarly[.]com
- grammarlyg[.]com
- grammarly2[.]com
- grammarlyl[.]com
- grammarly[.]work
- grammarlys[.]pro
- grammarly[.]site
- grammarly[.]kids
- grammarlyt[.]com
- grammarly[.]live
- 9grammarly[.]com
- grammarly[.]info
- grammarly[.]shop
- grammarly[.]blog

Cisco と Grammarly のブランド名を含む悪意あるドメインの例

- cisco[.]work
- cisco[.]asia
- cisco[.]pics
- ciscoway[.]cc
- ciscopro[.]ru
- shopcisco[.]eu
- mygrammarly[.]co
- grammarly[.]pics
- grammarlyget[.]com
- appgrammarly[.]info