Uncovering Other DarkTortilla Threat Vectors

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

As an age-old digital threat, phishing just continues to grow in sophistication over time, as DarkTortilla showed. Cyble Research and Intelligence Labs (CRIL) published a technical analysis of the threat specifically targeting Cisco and Grammarly. Are there other potential threat vectors, though?

WhoisXML API researchers obtained three indicators of compromise (IoCs) and performed an expansion analysis that led to the discovery of:

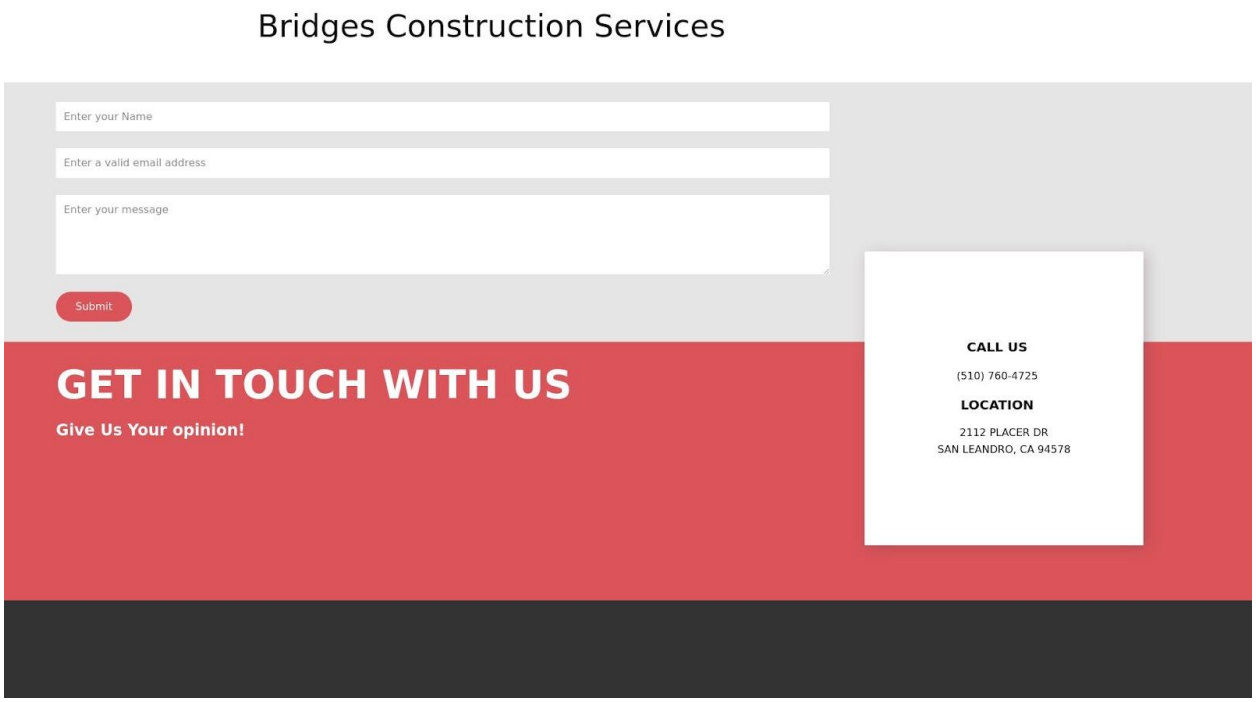
- Two IP addresses the domains resolved to
- 300+ domains that shared the IoCs' IP hosts, two of which were found malicious
- 11,358+ domains that contained the strings *Cisco*, *Grammarly*, or *Atomm* and could be used for other malicious campaigns; only 4% of these domains seemingly belonged to the legitimate companies and 23 were found malicious

DNS Ties

The CRIL report identified two domains—cicsom[.]com and gnammarly[.]com—and one URL—https://atomm[.]com[.]br/[.]well-known/acme-challenge/ol/Fjawtld[.]png—as IoCs.

DNS lookups for the IoCs allowed us to uncover two IP resolutions—104[.]21[.]15[.]248 and 172[.]67[.]165[.]88. Both IP addresses were geographically located in the U.S. and managed by Cloudflare, Inc.

Reverse IP lookups for these then led to the discovery of at least 300 potentially connected domains. A bulk malware check for these web properties revealed that two were malicious, namely, bridgesconstructionservicesinc[.]com and cl7q5s[.]cyou.



Screenshot of bridgesconstructionservicesinc[.]com

WHOIS Connections

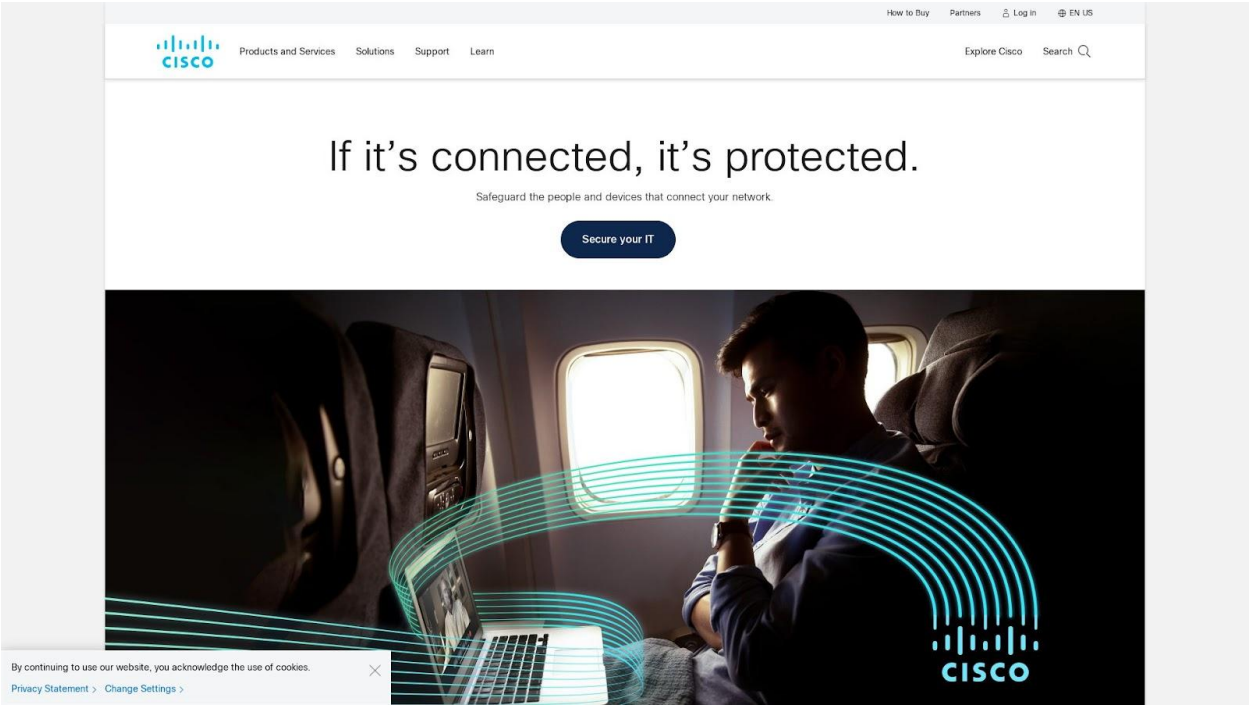
Since the phishers' targeted legitimate companies, we looked for other possible cybersquatting domains. We used the strings *Cisco*, *Grammarly*, and *Atomm* as Domains & Subdomains Discovery search terms to do that, though we only focused on looking for domains akin to the IoCs.

Our search uncovered at least 11,358 domains, 23 of which turned out to be malicious. In particular, 21 of these web properties seemingly served as malware hosts, one was a confirmed spam host, and another one was a confirmed phishing page. We named 10 of the malicious domains below.

MALICIOUS DOMAIN	CATEGORY
cisco[.]work	Malware
cisco[.]asia	Malware
cisco[.]pics	Malware
ciscopro[.]ru	Malware
shopcisco[.]eu	Malware

ciscoav[.]com	Phishing
grammarly[.]pics	Malware
grammarlyget[.]com	Malware
appgrammarly[.]info	Malware
mygrammarly[.]co	Spam

Apart from typosquatting on the companies' brands, some of the malicious domains also seemed to redirect to the organizations' legitimate pages. Here's an example obtained from a screenshot lookup.



Screenshot of cisco[.]pics that redirected to cisco[.]com

Next, we compared the 11,000+ potential cybersquatting domains' WHOIS records with those of the legitimate companies. Only 451 of them were owned by the imitated entities. Note that the comparisons were easy to do for Cisco since the organization didn't redact their WHOIS records. It wasn't as straightforward, however, for Grammarly that had a redacted WHOIS record.

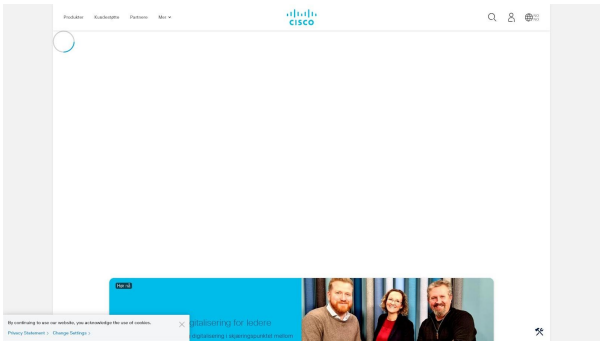
We had to use two filters for the Grammarly look-alike domains. First, we filtered out those that used a different registration organization other than *Domains By Proxy, LLC*. Next, we took out

the digital properties that indicated a registrar name other than *GoDaddy.com, LLC*. That left us with only 27 domains likely owned by Grammarly out of the total 476 that contained the company's brand name.

The table below shows the specific WHOIS record details we used to determine ownership.

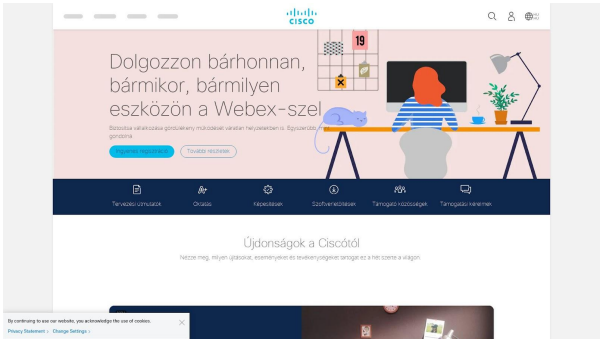
COMPANY	LEGITIMATE DOMAIN	WHOIS RECORD DETAIL USED AS COMPARISON PARAMETER
Cisco	cisco[.]com	**Administrative email address:** infosec@cisco[.]com
Grammarly	grammarly[.]com	**Registrant organization:** Domains By Proxy, LLC **Registrar name:** GoDaddy.com, LLC

We also obtained screenshots for look-alike domains that could serve as phishing pages or other malware distributors, assuming they did not redirect to other pages. Here are some examples of the suspicious web pages that didn't share the WHOIS record identifiers we used for Cisco and Grammarly.

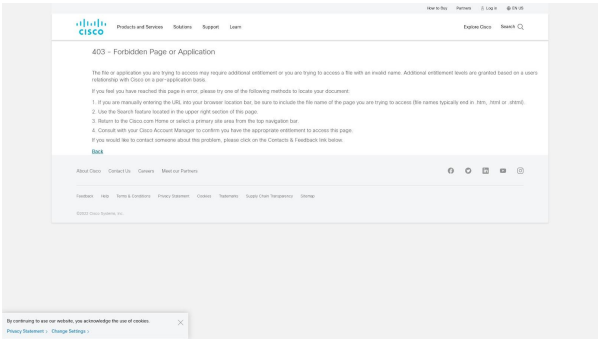


Screenshot of cisco[.]no

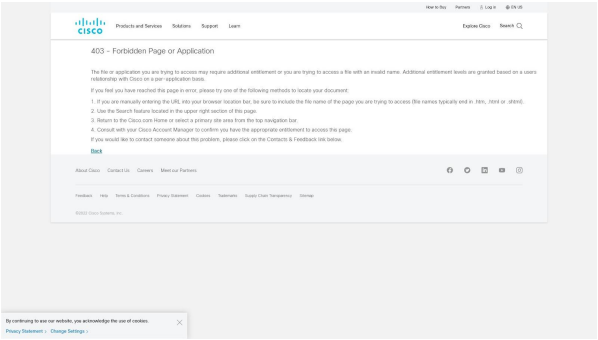
Screenshot of cisco[.]es



Screenshot of cisco[.]hu

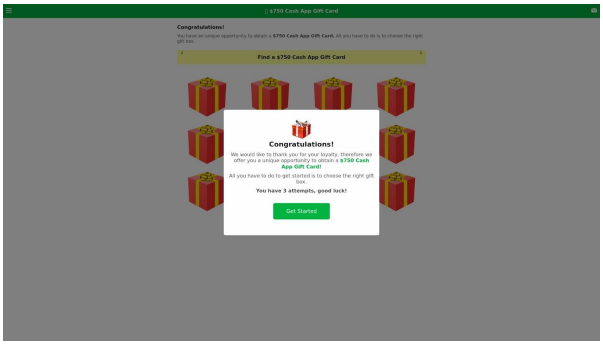


Screenshot of cisco[.]sn

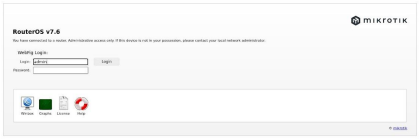


Screenshot of cisco[.]ug

And while the content of some of the look-alike domains didn't sport the spoofed companies' logos and content, they could easily trick visitors into giving out personal information, putting them in danger of getting phished or scammed. Examples of such suspicious domains hosting pages that offered prizes in exchange for playing a game or account login pages are shown below.



Screenshot of mygrammarly[.]co



Screenshot of grammarly[.]pics

—

Our IoC expansion analysis aided by IP, DNS, and WHOIS intelligence enabled us to uncover 11,600+ artifacts that could be connected to DarkTortilla. It also allowed us to identify 29 malicious domains that could particularly put Cisco or Grammarly customers at risk of spamming, phishing, and computer malware infection.

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

IoCs Identified by CRIL and AlienVault

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

IP Address Resolutions of the Domains Identified as IoCs

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

Sample Domains That Shared Some IoCs' IP Hosts

- a5t18ra2[.]top
- abchisilotyrel[.]tk
- abraajaula[.]com
- acaiteria19k[.]pwa[.]app[.]br
- acheizap[.]pwa[.]app[.]br
- acostafam[.]net
- admin[.]jonosheba[.]planetxinc[.]xyz
- adriaticreal[.]cz
- adtiojor[.]tk
- africanad[.]ca
- agencies[.]ticketyboo[.]cloud
- agle-pigina[.]vip
- ai[.]jaymcgrath[.]id[.]au
- aircylindertubes[.]today
- ajfheijdfj[.]cf
- akeyplan[.]com
- akgplb[.]com
- alaltalitalsma[.]tk
- alexandresa[.]com[.]br
- alhermayrmounchee[.]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

Malicious Domains That Shared Some IoCs' IP Hosts

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

Sample Domains That Contained the strings *Cisco*, *Grammarly*, or *Atomm* Brand Names

- 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

- ciscon[.]se
- scisco[.]it
- cisco[.]soy
- cisco[.]icu
- ciscon[.]cn
- ciscoo[.]be
- ciscos[.]fr
- ciscom[.]it
- ciscom[.]ro
- xn--csco-lza[.]com
- ciscoo[.]us
- ciscom[.]de
- ciscos[.]pw
- ciscoo[.]cn
- cisco1[.]tk
- ciscos[.]cn
- vcisco[.]de
- ciscos[.]eu
- cisco[.]one
- ciscod[.]vg
- ciscom[.]pk
- cisco[.]com
- cisco[.]bid
- scisco[.]se
- ciscos[.]us
- ciscon[.]eu
- xcisco[.]ru
- scisco[.]de
- ciscom[.]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
- ciscom[.]ch
- xn--csco-vw5a[.]com
- ncisco[.]es
- cisco[.]xxx
- ciscor[.]co
- ecisco[.]ro
- cisco0[.]tk
- 2cisco[.]ru
- xn--csco-vpa[.]com
- ciscor[.]de
- cisco[.]org
- xn--cico-rxb[.]com
- zcisco[.]cn
- ciscon[.]in
- cisco2[.]tk
- ycisco[.]cn
- ciscoo[.]ir
- cisco[.]mom
- xn--csco-5pa[.]com
- cisco[.]gdn
- cisco[.]frl
- ecisco[.]de
- 4cisco[.]ru
- tcisco[.]ru
- acisco[.]ml
- scisco[.]nl
- ciscon[.]be
- xn--csco-qpa[.]com
- ioe[.]cisco
- scisco[.]ca
- ciscom[.]ir
- ciscoo[.]ml
- scisco[.]co
- ciscom[.]cn
- ciscon[.]de
- cisco[.]ooo
- cisco[.]xin
- ciscos[.]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
- ciscol[.]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
- ciscon[.]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
- atommultiekspres[.]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--atommllreport-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

Sample Malicious Domains That Contained the Cisco and Grammarly Brand Names

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