Luxury Jewelry, Anyone? Watch Out for Fakes

Table of Contents

Executive Report

Scammers and counterfeiters are always on the lookout for quick gains. And the more expensive the fake item, the bigger the possible gain. It's no wonder then why they're looking to mimic the world's most popular luxury jewelers.

But companies aren't taking things sitting down. Cartier, for one, decided to fight back by filing lawsuits against knock-off sellers. Is Cartier the sole target, though? Our research findings clearly show it's not.

A closer look at the Domain Name System (DNS) trends for seven of the world's top luxury jewelers found:

- More than 8,200 domains and over 5,400 subdomains possibly mimicking the legitimate web properties of Cartier, Nadine Ghosn Fine Jewelry, Harry Winston, Messika, David Yurman, Monica Vinader, and Van Cleef & Arpels
- Less than 1% of the domains containing the top luxury jewelers' names could be publicly attributed to the companies
- More than 30 of the look-alike domains and subdomains have been dubbed "malicious" by various malware engines to date
- More than 140 of the domains' IP resolutions were deemed "malicious"

The World's Top Luxury Jewelers

Given Cartier's recent move to take the fight to scammers, we sought to determine if other luxury jewelers were also at risk. This study focused on seven companies that knock-off sellers may be trailing their sights on, namely, Cartier, Nadine Ghosn Fine Jewelry, Harry Winston, Messika, David Yurman, Monica Vinader, and Van Cleef & Arpels.

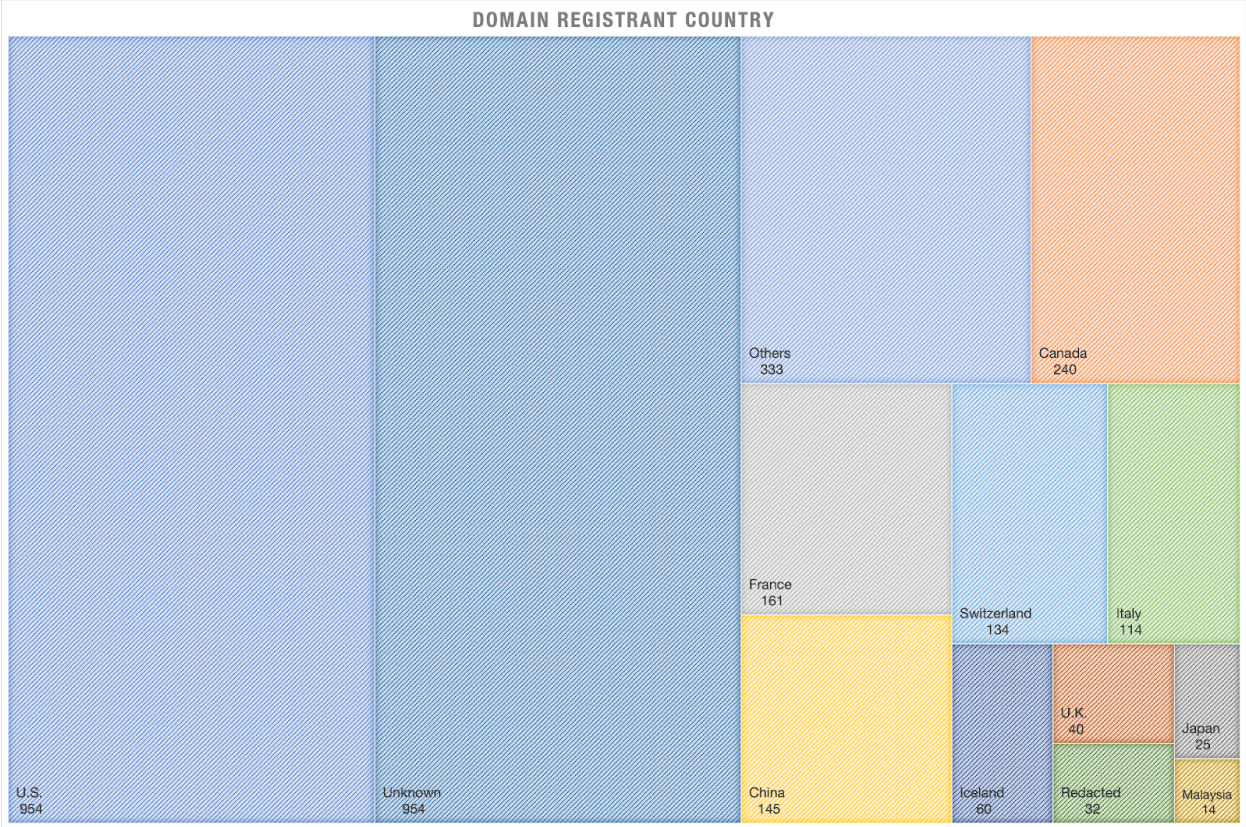
Are the Luxury Jewelers at Risk of Spoofing?

We first sought a variety of publicly available identifiers in WHOIS records (registrant email address, organization, or privacy protection provider) to attribute the look-alike web properties to the possibly mimicked jewelers. We also considered the domains' ages and registrant countries to weed out false positives.

We then used the following strings as search terms for Domains & Subdomains Discovery to look for potential fake pages.

Luxury Jeweler	Legitimate Domain	Registrant Country	String
Cartier	cartier[.]com	Switzerland	"cartier"
Nadine Ghosn Fine Jewelry	nadineghosn[.]com	U.S.	"nadineghosn"
Harry Winston	harrywinston[.]com	Switzerland	"harrywinston"
Messika	messika[.]com	France	"messika"
David Yurman	davidyurman[.]com	U.S.	"davidyurman"
Monica Vinader	monicavinader[.]com	U.K.	"monicavinader"
Van Cleef & Arpels	vancleefarpels[.]com	Switzerland	"vancleefarpels"

Our search led to the discovery of 8,229 domains and 5,406 subdomains. Of the more than 8,200 domains, only 45 shared the legitimate domain names' WHOIS record details. A majority of them named the U.S. as their registrant country while the remaining were distributed among 57 other nations. This is a far cry from the truth, as the spoofed companies only named four countries in their records—Switzerland, the U.S., France, and the U.K.



A Threat Intelligence Platform (TIP) malware check also showed that 26 of the look-alike domains and five of the look-alike subdomains were malicious.

It's also interesting to note that several of the malicious Cartier domain look-alikes that sport country name abbreviations like cartieruk[.]com differs from the legitimate local U.K. page, which uses a ccTLD as in cartier[.]com/en-gb/.

Further scrutiny of the subdomains, meanwhile, revealed commonly used strings topped by "watch," "blog," "jewel," "shop," "outlet," "cheap," "swiss," "buy," "time," and "fashion."

A bulk IP geolocation lookup for the potential look-alike domains showed that they resolved to 1,940 unique IP addresses, 148 of which were malware hosts according to TIP.

—

Buyers eyeing to purchase luxury jewelry should be especially wary of ending up on the many fake websites touting more affordable products. They're likely to end up with counterfeit goods or have their personal details robbed.

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 Domains Containing the Names of the Top Luxury Jewelers

- cartier-cartier[.]xn--kprw13d
- cartier-cartier[.]uk
- cartiercartier[.]com
- cartier-cartiers[.]cn
- cartiercartieros[.]gq
- cartierscartier[.]com
- cartier-cartier[.]co[.]uk
- cartierbycartier[.]store
- cartier-cartier[.]nom[.]za
- cartier[.]pw
- cartier[.]kz
- cartier[.]im

- cartier[.]dk
- cartier[.]md
- cartier[.]fr
- cartier[.]ua
- cartier[.]xn--ses554g
- cartier[.]in
- cartier[.]es
- cartier[.]lk
- nadineghosn[.]cn
- nadineghosn[.]com
- nadineghosn[.]xyz
- nadineghosn[.]top
- nadineghosn[.]info
- nadineghosn[.]design
- nadineghosngems[.]com
- nadineghosnjewels[.]com
- nadineghosndesign[.]com
- nadineghosnjewelry[.]net
- nadineghosnjewelry[.]com
- nadineghosngallery[.]com
- nadineghosncollection[.]com
- nadineghosnjewelry[.]online
- harrywinston[.]uk
- harrywinston[.]in
- harrywinston[.]sg
- harrywinston[.]tm
- harrywinston[.]su
- harrywinston[.]cf
- harrywinston[.]mx
- harrywinston[.]re
- harrywinston[.]tv
- harrywinston[.]de
- harrywinston[.]vn
- harrywinston[.]sc
- harrywinston[.]ms
- harrywinston[.]cr
- harrywinston[.]es
- messika[.]sa
- messika[.]cn
- messika[.]se
- messika[.]tw
- messika[.]gr
- messika[.]hr
- messika[.]lv
- messika[.]es
- messika[.]kr
- messika[.]pt
- messika[.]ma
- messika[.]at
- messika[.]co
- messika[.]lt
- messika[.]qa
- davidyurman[.]cn
- davidyurman[.]nl
- davidyurman[.]uk
- davidyurman[.]se
- davidyurman[.]us
- davidyurman[.]tv
- davidyurman[.]ca
- davidyurman[.]jp
- davidyurman[.]cc
- davidyurman[.]be
- davidyurman[.]ru
- davidyurman[.]tw
- davidyurman[.]it
- davidyurman[.]at
- monicavinader[.]mo
- monicavinader[.]eu
- monicavinader[.]uk
- monicavinader[.]ca
- monicavinader[.]ru
- monicavinader[.]gr
- monicavinader[.]be
- monicavinader[.]qa
- monicavinader[.]it
- monicavinader[.]pt

- monicavinader[.]es
- monicavinader[.]at
- monicavinader[.]sg
- monicavinader[.]ae
- vancleefarpels[.]xn--kprw13d
- vancleefarpels[.]it
- vancleefarpels[.]ca
- vancleefarpels[.]cn
- vancleefarpels[.]tk
- vancleefarpels[.]es
- vancleefarpels[.]uk
- vancleefarpels[.]co
- vancleefarpels[.]in

Sample Malicious Possibly Connected Domains

- cartierjl[.]com
- cartieruk[.]com
- cartier168[.]com
- hotcartier[.]com
- cartier-tw[.]com
- cartiertour[.]com
- jerseycartier[.]xyz
- cartierreplica[.]net
- iswearcartier[.]work
- bitcoincartier[.]org
- cartierreplica[.]top
- cartierbracelet[.]cc
- aaacartierwatches[.]cn
- buycartieronline[.]com
- cartierlovestore[.]xyz
- topreplicacartier[.]cn
- cartierapartenope[.]it
- cartierloveonline[.]com
- cartierwheelhouse[.]org
- cartierwatchescom[.]com

Sample Subdomains Containing the Names of Top Luxury Jewelers

- lecartier[.]lecartier[.]pmdms[.]com
- cartier[.]axiangshui[.]com
- cartier[.]cnam[.]fr
- cartier[.]dyzqmdgeb[.]cn
- cartier[.]ezinemark[.]com
- cartier[.]izawan[.]com
- cartier[.]kanashibari[.]jp
- cartier[.]68q1r9[.]cn
- cartier[.]flont[.]com
- cartier[.]ihcss3[.]cn
- harrywinston[.]seesaa[.]net
- harrywinston[.]portal[.]gold
- harrywinston[.]luxoria[.]com[.]ua
- harrywinston[.]continentaltravelgroup[.]com
- harrywinston[.]watchescopy[.]net
- harrywinston[.]v-kei[.]net
- harrywinston[.]wosjy[.]com
- harrywinston[.]1pinyuqi[.]com
- harrywinston[.]itita[.]com
- harrywinston[.]xingter[.]com
- messika[.]cdn-tech[.]io
- messika[.]volleto[.]com
- messika[.]lestudiopry[.]com
- messika[.]654[.]co[.]il
- messika[.]on3cx[.]fr
- messika[.]b2bylon[.]tech
- messika[.]polyvore[.]com
- messika[.]antho-web[.]com
- messika[.]deviantart[.]com
- messika[.]my3cx[.]fr
- davidyurman[.]savesmarts[.]com

- davidyurman[.]wow-deal[.]com
- davidyurman[.]polyvore[.]com
- davidyurman[.]brickworksoftware[.]com
- davidyurman[.]hellosociety[.]co
- davidyurman[.]knoji[.]com
- davidyurman[.]weebly[.]com
- davidyurman[.]loopsb[.]net
- davidyurman[.]createthe[.]com
- davidyurman[.]robling[.]io
- monicavinader[.]polyvore[.]com
- monicavinader[.]cafe24[.]com
- monicavinader[.]mention-me[.]com
- monicavinader[.]tooskan[.]com
- monicavinader[.]gappt[.]com
- monicavinader[.]knoji[.]com
- monicavinader2[.]d3r-cdn[.]com
- monicavinader[.]freshdesk[.]com
- monicavinaders[.]campghana[.]org
- m[.]monicavinader[.]cafe24[.]com
- cartier[.]tech[.]blog
- cartier[.]elle[.]ru
- cartier[.]trimp[.]biz
- cartier[.]ateliertnc[.]com
- cartier[.]menparfums[.]us
- cartier[.]techplatforms[.]ca
- cartier[.]health[.]blog
- vancleefarpels[.]zhaohuangjin[.]com
- vancleefarpels[.]granadis[.]com
- vancleefarpels[.]itita[.]com
- vancleefarpels[.]us[.]org
- vancleefarpels[.]dlosri[.]com
- vancleefarpels[.]21512[.]com
- vancleefarpels[.]v-boutique[.]com
- vancleefarpels[.]creativecreation[.]biz
- vancleefarpels[.]ru[.]com
- www[.]vancleefarpels[.]us[.]com
- cartier[.]ke22p[.]cn
- cartier[.]nabebugyou[.]com
- cartier[.]novista[.]rs
- cartier[.]outlet-bargain[.]net
- cartier[.]jinpeng58[.]com
- cartier[.]m05[.]biz
- cartier[.]tyanoyu[.]net
- cartier[.]ucmerced[.]edu
- cartier[.]viptime[.]com[.]ua
- cartier[.]chinaspvcom[.]cn
- cartier[.]strat-scl[.]com
- cartier[.]aam-com[.]com
- cartier[.]chimanako[.]net
- cartier[.]datasuns[.]com[.]cn
- cartier[.]dflgms[.]cn
- cartier[.]mercurioimaging[.]com

Malicious Possibly Connected Subdomains

- cartierenterprises[.]study-bright[.]com
- cartierassociates[.]study-bright[.]com
- www[.]cartierassociates[.]study-bright[.]com
- www[.]cartierenterprises[.]study-bright[.]com
- culminating-assignment-cartier[.]335604930[.]repl[.]co

Sample Domain IP Resolutions

- 129[.]227[.]251[.]80
- 34[.]202[.]63[.]170
- 130[.]211[.]40[.]170
- 78[.]31[.]111[.]139
- 31[.]31[.]205[.]163
- 81[.]56[.]240[.]150
- 23[.]77[.]64[.]181
- 2a02[:]4780[:]9[:]607[:]0[:]2775[:]dc8e[:]2
- 45[.]84[.]205[.]195
- 195[.]234[.]224[.]176
- 23[.]77[.]64[.]243
- 64[.]190[.]63[.]111
- 2606[:]4700[:]3031[::]ac43[:]c87c
- 2606[:]4700[:]3033[::]6815[:]3a33
- 104[.]21[.]58[.]51
- 172[.]67[.]200[.]124
- 212[.]44[.]112[.]34
- 2402[:]7d80[:]fffc[::]27
- 45[.]120[.]243[.]27
- 34[.]102[.]136[.]180
- 2a01[:]5b40[:]0[:]bc03[::]1
- 185[.]134[.]245[.]113
- 31[.]171[.]152[.]93
- 31[.]217[.]196[.]220
- 138[.]68[.]115[.]136
- 103[.]243[.]253[.]190
- 52[.]8[.]174[.]221
- 172[.]252[.]99[.]102
- 3[.]64[.]163[.]50
- 103[.]120[.]83[.]111
- 194[.]206[.]126[.]204
- 103[.]120[.]83[.]249
- 2607[:]f1c0[:]100f[:]f000[::]2ca
- 74[.]208[.]236[.]153
- 95[.]168[.]169[.]96
- 185[.]179[.]189[.]71
- 213[.]186[.]33[.]5
- 51[.]161[.]122[.]130
- 43[.]130[.]65[.]190
- 46[.]105[.]99[.]143
- 173[.]209[.]38[.]35
- 2a00[:]d70[:]0[:]a[::]166
- 217[.]26[.]48[.]101
- 2606[:]4700[:]3035[::]6815[:]502c
- 2606[:]4700[:]3037[::]ac43[:]ae13
- 104[.]21[.]80[.]44
- 172[.]67[.]174[.]19
- 15[.]197[.]142[.]173
- 3[.]33[.]152[.]147
- 193[.]39[.]9[.]155
- 2606[:]4700[:]3035[::]6815[:]2942
- 2606[:]4700[:]3032[::]ac43[:]bdc4
- 104[.]21[.]41[.]66
- 172[.]67[.]189[.]196
- 46[.]37[.]17[.]19
- 103[.]120[.]80[.]144
- 2606[:]4700[:]3034[::]ac43[:]bc71
- 2606[:]4700[:]3035[::]6815[:]871
- 172[.]67[.]188[.]113
- 104[.]21[.]8[.]113
- 54[.]36[.]120[.]161
- 89[.]31[.]143[.]1
- 217[.]70[.]184[.]38
- 2a02[:]5b41[:]4[:]401[::]7
- 194[.]32[.]152[.]8
- 2a01[:]4f8[:]1c17[:]fa73[::]1
- 142[.]132[.]181[.]81
- 173[.]249[.]10[.]41
- 217[.]160[.]0[.]73

- 103[.]139[.]0[.]32
- 103[.]120[.]80[.]155
- 2607[:]5300[:]203[:]3f32[::]
- 54[.]39[.]128[.]50
- 66[.]45[.]246[.]141
- 52[.]214[.]231[.]129
- 81[.]88[.]48[.]71
- 50[.]62[.]139[.]112
- 129[.]227[.]61[.]147
- 80[.]74[.]158[.]35
- 66[.]81[.]199[.]56
- 198[.]49[.]23[.]144
- 198[.]49[.]23[.]145
- 198[.]185[.]159[.]144
- 198[.]185[.]159[.]145
- 185[.]230[.]63[.]186
- 185[.]230[.]63[.]107
- 185[.]230[.]63[.]171
- 156[.]238[.]106[.]190
- 216[.]243[.]142[.]37
- 173[.]208[.]137[.]3
- 129[.]227[.]251[.]86
- 129[.]227[.]251[.]107
- 2001[:]41d0[:]301[::]29
- 51[.]91[.]236[.]255
- 104[.]247[.]82[.]174
- 45[.]194[.]220[.]2
- 2606[:]4700[:]3034[::]ac43[:]af26
- 2606[:]4700[:]3036[::]6815[:]3004
- 104[.]21[.]48[.]4
- 172[.]67[.]175[.]38

Sample Malicious IP Addresses

- 130[.]211[.]40[.]170
- 34[.]102[.]136[.]180
- 31[.]217[.]196[.]220
- 3[.]64[.]163[.]50
- 213[.]186[.]33[.]5
- 217[.]26[.]48[.]101
- 89[.]31[.]143[.]1
- 217[.]70[.]184[.]38
- 103[.]139[.]0[.]32
- 103[.]120[.]80[.]155
- 66[.]45[.]246[.]141
- 51[.]91[.]236[.]255
- 72[.]52[.]179[.]174
- 104[.]247[.]82[.]54
- 87[.]98[.]154[.]146
- 45[.]33[.]2[.]79
- 45[.]79[.]19[.]196
- 213[.]186[.]33[.]19
- 45[.]88[.]202[.]115
- 94[.]136[.]40[.]82
- 192[.]254[.]237[.]106
- 159[.]89[.]244[.]183
- 150[.]95[.]255[.]38
- 162[.]241[.]218[.]163
- 207[.]148[.]248[.]143
- 34[.]98[.]99[.]30
- 72[.]167[.]191[.]69
- 35[.]172[.]94[.]1
- 195[.]110[.]124[.]133
- 95[.]128[.]74[.]25
- 185[.]114[.]245[.]109
- 205[.]178[.]189[.]129
- 198[.]57[.]247[.]153
- 217[.]160[.]0[.]78
- 75[.]2[.]18[.]233
- 72[.]52[.]179[.]175
- 45[.]79[.]222[.]138
- 172[.]65[.]227[.]72

- 23[.]202[.]231[.]167
- 5[.]157[.]87[.]204
- 213[.]171[.]195[.]105
- 162[.]255[.]119[.]181
- 178[.]63[.]41[.]150
- 88[.]198[.]29[.]97
- 208[.]91[.]197[.]22
- 64[.]98[.]145[.]30
- 192[.]0[.]78[.]24
- 81[.]169[.]145[.]165
- 108[.]179[.]229[.]36
- 213[.]186[.]33[.]87