

Using the Silent Push app and API to find punycode domains

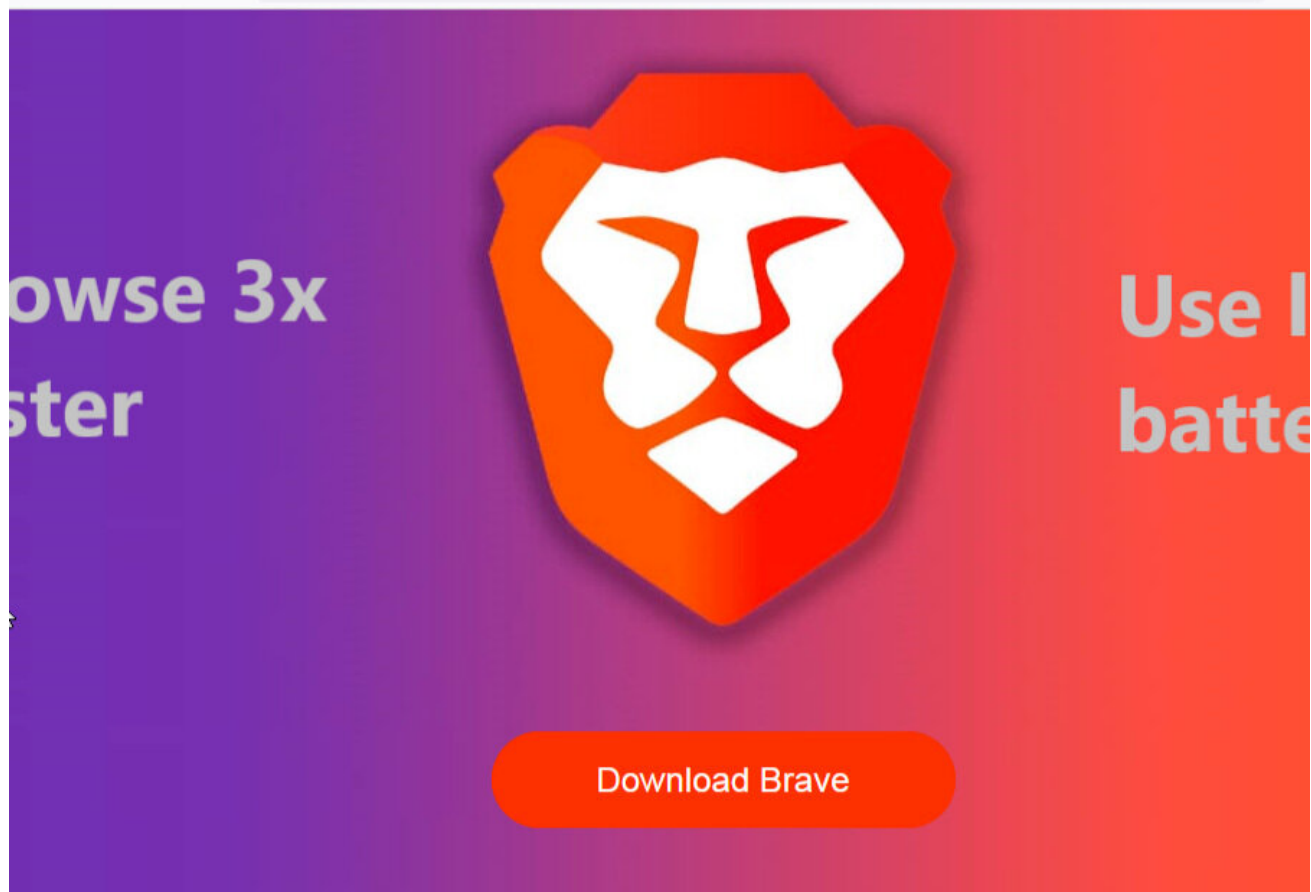
 silentpush.com/blog/using-the-silent-push-app-and-api-to-find-punycode-domains

July 29, 2021



Jul 29

Written By [Martijn Grooten](#)



Yesterday, Yan Zhu, a security engineer for the privacy-focused Brave web browser, [tweeted](#) about a domain impersonating Brave that was promoted through Google ads.

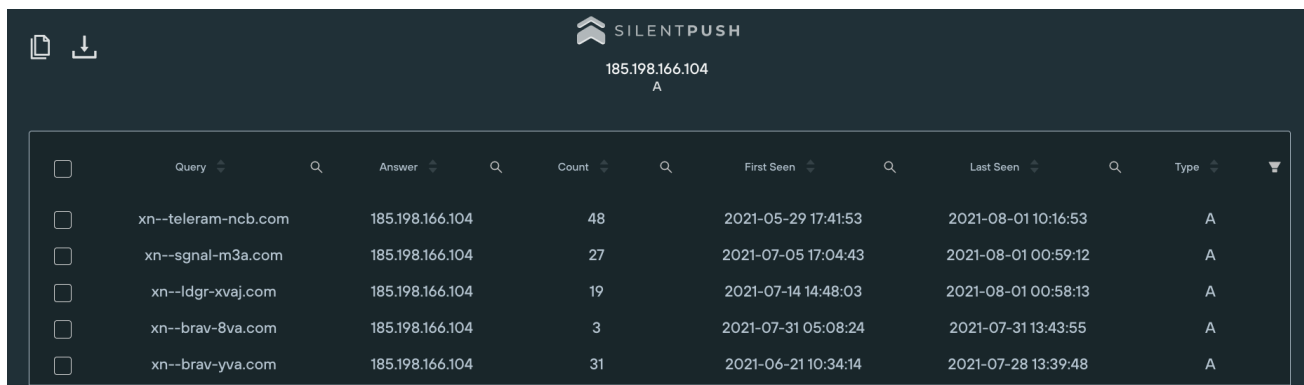
The domain was [bravè.com](#). Note the accent on the e, which distinguishes it from [brave.com](#), the domain it was impersonating.

This is an example of an [Internationalized Domain Name \(IDN\)](#), a domain name that includes non-ASCII characters. Such domains have an ASCII representation that starts with [xn--](#) and use [punycode](#) to convert from ASCII to unicode and vice versa. The ASCII representation of the impersonating domain is [xn--brav-yva.com](#).

When IDNs are used to impersonate existing domains, one speaks of a homograph or homoglyph attack. Other than the use of accents on Latin characters, this also includes using similar-looking characters from non-Latin alphabets, such as using the Greek α instead of the Latin a. Though not incredibly common in practice, such attacks do exist and security researchers have warned about them for more than a decade.

The `bravè.com` or `xn--brav-yva.com` domain was registered through NameCheap in June and is hosted at `185.198.166.104`, which belongs to ITLDC, a Bulgarian cloud provider with servers in a number of countries.

My first thought was to use the Silent Push app to see what else is hosted there.



Query	Answer	Count	First Seen	Last Seen	Type
xn--teleram-ncb.com	185.198.166.104	48	2021-05-29 17:41:53	2021-08-01 10:16:53	A
xn--sgnal-m3a.com	185.198.166.104	27	2021-07-05 17:04:43	2021-08-01 00:59:12	A
xn--ldgr-xvaj.com	185.198.166.104	19	2021-07-14 14:48:03	2021-08-01 00:58:13	A
xn--brav-8va.com	185.198.166.104	3	2021-07-31 05:08:24	2021-07-31 13:43:55	A
xn--brav-yva.com	185.198.166.104	31	2021-06-21 10:34:14	2021-07-28 13:39:48	A

I found three more domain names, all IDNs: `xn--ldgr-xvaj.com`, `xn--sgnal-m3a.com` and `xn--teleram-ncb.com`. The unicode representations of these domains are `lędgër.com`, `signal.com` and `telegram.com` respectively, presumably impersonating cryptocurrency wallet maker Ledger and messaging apps Signal and Telegram. (I say 'presumably' because `signal.com` and `telegram.com` aren't actually linked to the respective messaging apps.)

These other three domains were also registered at NameCheap. Using our passive DNS, I found that none of the domains had been seen at another IP address, so I couldn't pivot any further.

However, I wondered if this actor could have hosted other domains at a different server. Assuming they'd also use the same registrar and hosting provider, I ran a search query in Silent Push's API for domains starting with `xn--` using NameCheap's name servers and hosted on ITLDC's ASN (AS21100).

I found nine further domains. Two of them (`xn--80aaw7ah.com` and `xn--80ahcbumt.org`) represent words in the Cyrillic alphabet and there is no reason to assume they are used for anything malicious.

The other seven, however, were all hosted on the same IP address (`195.245.113.25`) and all impersonate legitimate products, including once again Brave and Telegram:

SILENTPUSH
195.245.113.25
A

<input type="checkbox"/>	Query	Answer	Count	First Seen	Last Seen	Type
<input type="checkbox"/>	clubhousejoin.xyz	195.245.113.25	16	2021-02-15 21:57:58	2021-03-03 21:45:25	A
<input type="checkbox"/>	dplynews.xyz	195.245.113.25	233	2020-12-28 23:47:19	2021-08-01 06:26:26	A
<input type="checkbox"/>	globalnesx.xyz	195.245.113.25	166	2021-01-29 15:44:35	2021-08-01 06:27:17	A
<input type="checkbox"/>	improvedownload.club	195.245.113.25	79	2020-12-27 10:25:14	2021-01-29 10:28:00	A
<input type="checkbox"/>	opautoclicker.xyz	195.245.113.25	113	2021-03-08 17:38:12	2021-07-31 09:57:35	A
<input type="checkbox"/>	xn--brav-eva.com	195.245.113.25	90	2021-03-26 14:57:16	2021-07-29 00:35:13	A
<input type="checkbox"/>	xn--flightsimulator-mdc.com	195.245.113.25	110	2021-03-09 21:28:36	2021-07-29 00:35:28	A
<input type="checkbox"/>	xn--screncast-ehb.com	195.245.113.25	118	2021-03-07 21:27:23	2021-07-29 00:36:19	A
<input type="checkbox"/>	xn--ttelegram-w7a.com	195.245.113.25	45	2021-03-10 03:34:21	2021-05-03 18:26:43	A
<input type="checkbox"/>	xn--torbrowser-zxb.com	195.245.113.25	116	2021-03-12 21:10:37	2021-07-28 13:40:15	A
<input type="checkbox"/>	xn--tradingview-8sb.com	195.245.113.25	140	2021-02-15 15:07:27	2021-07-31 10:37:26	A
<input type="checkbox"/>	xn--xodus-hza.com	195.245.113.25	93	2021-04-05 18:43:30	2021-07-28 13:40:26	A

The fake installer on brave.com that prompted this research was an [ISO file](#) that appears to contain a version of the [Redline infostealer](#). That suggests it may be related to a [campaign](#) analysed by Morphisec last month, where Redline was also served packed inside an ISO through malicious Google ads, impersonating Telegram and other services. The domain names involved in that campaign were also registered through NameCheap.

As for IDNs, there are [tools](#) that help one find homograph attacks on an existing domain name. However, it is through a comprehensive and easily searchable passive DNS database that one can find a bigger picture of the campaign using a homograph attack.

Indicators

xn--brav-eva.com

xn--brav-yva.com

xn--flightsimulator-mdc.com

xn--ldgr-xvaj.com

xn--screncast-ehb.com

xn--sgnal-m3a.com

xn--teleram-ncb.com

xn--ttelegram-w7a.com

xn--torbrowser-zxb.com

xn--tradingview-8sb.com

xn--xodus-hza.com

185.198.166.104

195.245.113.25

Name *

Thank you!

Martijn Grooten