

OUT OF CHARACTER: USE OF PUNYCODE AND HOMOGLYPH ATTACKS TO OBFUSCATE URLS FOR PHISHING

Adrian Crenshaw



About Adrian

- ▣ I run Irongeek.com
- ▣ I have an interest in InfoSec education
- ▣ I don't know everything - I'm just a geek with time on my hands
- ▣ I'm an (Ir)regular on the InfoSec Daily Podcast:
<http://isdpodcast.com>
- ▣ Sr. Information Security Engineer at a Fortune 1000
- ▣ Co-Founder of Derbycon
<http://www.derbycon.com/>

Twitter: @Irongeek_ADC



Classic Phishing Obfuscations

- ▣ Would you follow a link in email to AdriansHouseOfPwnage.com?
- ▣ Text says one thing, link says another:
`<a href="http://irongeek.com">http://www.microsoft.com</a>`
- ▣ Confuse user with credentials section of a URL:
`http://www.microsoft.com@irongeek.com`
 - Firefox pops up a warning
 - IE just refuses to connect
- ▣ Other ideas?



Homographs

- ▣ Homographs = words that looks the same
- ▣ Homoglyphs = characters that look the same
- ▣ Examples:
 - rnicrosoft.com vs. microsoft.com
 - paypa1.com vs. paypal.com
 - IRONGEEK.COM vs. IRONGEEK.COM
- ▣ Now, what about Unicode?



Unicode

- ▣ ASCII only covers so many characters, but what about characters from other languages/scripts?
- ▣ Unicode to the rescue
 - 1,114,112 code points in the range 0 to 10FFFF
 - Mapped to common languages with room to expand
 - Different encoding styles (UTF-8, UTF-16, etc.)
 - 0–127 of UTF-8 match ASCII
 - Windows-1252 uses printable characters for 80 to 9F instead of control characters like ISO-8859-1
 - Commonly seen when “smart quotes” screw up



Problem: DNS is ASCII

- ▣ DNS labels (the parts separated by dots) follow the LDH rule:
 - Letters
 - Digits
 - Hyphen
- ▣ This would not allow for international characters in DNS labels
- ▣ Enter Punycode and IDNA



IDNA

- ▣ Internationalized Domain Names in Applications (IDNA) allows non-ASCII characters in the host section of a URL to map to DNS host names

café.com = xn--caf-dma.com

北京大学.中國 = xn--1lq90ic7fzpc.xn--fiqz9s



What about Homoglyphs in Unicode?

There are homoglyphs in Unicode that look the same as normal Latin characters, and these could be used for spoofing names, examples:

google.com = xn--googl-3we.com

(e is a Cyrillic small letter ie U+0435)

iucu.org = xn--ucU+ihd.org

(i is a Cyrillic small letter Byelorussian-Ukrainian i U+0456)

paypal.com = xn--pypal-4ve.com

(2nd a is Cyrillic small letter a U+0430)



Likely Sources for Homoglyphs

- ▣ Cyrillic script: а, с, е, о, р, х and у
- ▣ Latin alphabet appears twice, U+0021-007E (Basic Latin) & U+FF01-FF5E (Full width Latin):
!"\$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ
VWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
- ▣ Even some slashes
/(U+002f),/(U+0338),/(U+2044),/(U+2215),/
(U+2571), /, (U+ff0f)/, (U+ff89)



Slashes?

- ▣ Can other domains be used?
- ▣ `www.microsoft.com/index.html.irongeek.com`
Slash is U+2044



Homoglyph Attack Generator Demo

<http://www.irongeek.com/homoglyph-attack-generator.php>

Combination of JavaScript and PHP libraries created by phlyLabs
as part of phlyMail



Protections Implemented by Browsers

Firefox (11) shows Punycode if

▣ Not in TLD White List (about:config→network.IDN.whitelist)

.ac, .ar, .asia, .at, .biz, .br, .cat, .ch, .cl, .cn, .de, .dk, .ee, .es, .fi, .gr, .hu, .il, .info, .io, .ir, .is, .jp, .kr, .li, .lt, .lu, .lv, .museum, .no, .nu, .nz, .org, .pl, .pr, .se, .sh, .si, .tel, .th, .tm, .tw, .ua, .vn, .xn--0zwm56d, .xn--11b5bs3a9aj6g, .xn--80akhbyknj4f, .xn--90a3ac, .xn--9t4b11yi5a, .xn--deba0ad, .xn--fiqs8s, .xn--fiqz9s, .xn--fzc2c9e2c, .xn--g6w251d, .xn--hgbk6aj7f53bba, .xn--hlcj6aya9esc7a, .xn--j6w193g, .xn--jxalpdip, .xn--kgbechtv, .xn--kprw13d, .xn--kpry57d, .xn--mgba3a4f16a, .xn--mgba3a4fra, .xn--mgbaam7a8h, .xn--mgbayh7gpa, .xn--mgberp4a5d4a87g, .xn--mgberp4a5d4ar, .xn--mgbqly7c0a67fbc, .xn--mgbqly7cvafr, .xn--o3cw4h, .xn--ogbpf8fl, .xn--p1ai, .xn--wgbh1c, .xn--wgbl6a, .xn--xkc2al3hye2a, .xn--zckzah

☒network.IDN_show_punycode set to true (default false)

☐ Any of these blacklisted characters appear:

$\frac{1}{4}\frac{1}{2}\frac{3}{4}!$ $\frac{7}{8}$ $\frac{1}{2}$ $\frac{3}{4}$ $\frac{5}{6}$ $\frac{7}{8}$ $\frac{9}{10}$ $\frac{11}{12}$ $\frac{13}{14}$ $\frac{15}{16}$ $\frac{17}{18}$ $\frac{19}{20}$ $\frac{21}{22}$ $\frac{23}{24}$ $\frac{25}{26}$ $\frac{27}{28}$ $\frac{29}{30}$ $\frac{31}{32}$ $\frac{33}{34}$ $\frac{35}{36}$ $\frac{37}{38}$ $\frac{39}{40}$ $\frac{41}{42}$ $\frac{43}{44}$ $\frac{45}{46}$ $\frac{47}{48}$ $\frac{49}{50}$ $\frac{51}{52}$ $\frac{53}{54}$ $\frac{55}{56}$ $\frac{57}{58}$ $\frac{59}{60}$ $\frac{61}{62}$ $\frac{63}{64}$ $\frac{65}{66}$ $\frac{67}{68}$ $\frac{69}{70}$ $\frac{71}{72}$ $\frac{73}{74}$ $\frac{75}{76}$ $\frac{77}{78}$ $\frac{79}{80}$ $\frac{81}{82}$ $\frac{83}{84}$ $\frac{85}{86}$ $\frac{87}{88}$ $\frac{89}{90}$ $\frac{91}{92}$ $\frac{93}{94}$ $\frac{95}{96}$ $\frac{97}{98}$ $\frac{99}{100}$ $\frac{101}{102}$ $\frac{103}{104}$ $\frac{105}{106}$ $\frac{107}{108}$ $\frac{109}{110}$ $\frac{111}{112}$ $\frac{113}{114}$ $\frac{115}{116}$ $\frac{117}{118}$ $\frac{119}{120}$ $\frac{121}{122}$ $\frac{123}{124}$ $\frac{125}{126}$ $\frac{127}{128}$ $\frac{129}{130}$ $\frac{131}{132}$ $\frac{133}{134}$ $\frac{135}{136}$ $\frac{137}{138}$ $\frac{139}{140}$ $\frac{141}{142}$ $\frac{143}{144}$ $\frac{145}{146}$ $\frac{147}{148}$ $\frac{149}{150}$ $\frac{151}{152}$ $\frac{153}{154}$ $\frac{155}{156}$ $\frac{157}{158}$ $\frac{159}{160}$ $\frac{161}{162}$ $\frac{163}{164}$ $\frac{165}{166}$ $\frac{167}{168}$ $\frac{169}{170}$ $\frac{171}{172}$ $\frac{173}{174}$ $\frac{175}{176}$ $\frac{177}{178}$ $\frac{179}{180}$ $\frac{181}{182}$ $\frac{183}{184}$ $\frac{185}{186}$ $\frac{187}{188}$ $\frac{189}{190}$ $\frac{191}{192}$ $\frac{193}{194}$ $\frac{195}{196}$ $\frac{197}{198}$ $\frac{199}{200}$ $\frac{201}{202}$ $\frac{203}{204}$ $\frac{205}{206}$ $\frac{207}{208}$ $\frac{209}{210}$ $\frac{211}{212}$ $\frac{213}{214}$ $\frac{215}{216}$ $\frac{217}{218}$ $\frac{219}{220}$ $\frac{221}{222}$ $\frac{223}{224}$ $\frac{225}{226}$ $\frac{227}{228}$ $\frac{229}{230}$ $\frac{231}{232}$ $\frac{233}{234}$ $\frac{235}{236}$ $\frac{237}{238}$ $\frac{239}{240}$ $\frac{241}{242}$ $\frac{243}{244}$ $\frac{245}{246}$ $\frac{247}{248}$ $\frac{249}{250}$ $\frac{251}{252}$ $\frac{253}{254}$ $\frac{255}{256}$ $\frac{257}{258}$ $\frac{259}{260}$ $\frac{261}{262}$ $\frac{263}{264}$ $\frac{265}{266}$ $\frac{267}{268}$ $\frac{269}{270}$ $\frac{271}{272}$ $\frac{273}{274}$ $\frac{275}{276}$ $\frac{277}{278}$ $\frac{279}{280}$ $\frac{281}{282}$ $\frac{283}{284}$ $\frac{285}{286}$ $\frac{287}{288}$ $\frac{289}{290}$ $\frac{291}{292}$ $\frac{293}{294}$ $\frac{295}{296}$ $\frac{297}{298}$ $\frac{299}{300}$ $\frac{301}{302}$ $\frac{303}{304}$ $\frac{305}{306}$ $\frac{307}{308}$ $\frac{309}{310}$ $\frac{311}{312}$ $\frac{313}{314}$ $\frac{315}{316}$ $\frac{317}{318}$ $\frac{319}{320}$ $\frac{321}{322}$ $\frac{323}{324}$ $\frac{325}{326}$ $\frac{327}{328}$ $\frac{329}{330}$ $\frac{331}{332}$ $\frac{333}{334}$ $\frac{335}{336}$ $\frac{337}{338}$ $\frac{339}{340}$ $\frac{341}{342}$ $\frac{343}{344}$ $\frac{345}{346}$ $\frac{347}{348}$ $\frac{349}{350}$ $\frac{351}{352}$ $\frac{353}{354}$ $\frac{355}{356}$ $\frac{357}{358}$ $\frac{359}{360}$ $\frac{361}{362}$ $\frac{363}{364}$ $\frac{365}{366}$ $\frac{367}{368}$ $\frac{369}{370}$ $\frac{371}{372}$ $\frac{373}{374}$ $\frac{375}{376}$ $\frac{377}{378}$ $\frac{379}{380}$ $\frac{381}{382}$ $\frac{383}{384}$ $\frac{385}{386}$ $\frac{387}{388}$ $\frac{389}{390}$ $\frac{391}{392}$ $\frac{393}{394}$ $\frac{395}{396}$ $\frac{397}{398}$ $\frac{399}{400}$ $\frac{401}{402}$ $\frac{403}{404}$ $\frac{405}{406}$ $\frac{407}{408}$ $\frac{409}{410}$ $\frac{411}{412}$ $\frac{413}{414}$ $\frac{415}{416}$ $\frac{417}{418}$ $\frac{419}{420}$ $\frac{421}{422}$ $\frac{423}{424}$ $\frac{425}{426}$ $\frac{427}{428}$ $\frac{429}{430}$ $\frac{431}{432}$ $\frac{433}{434}$ $\frac{435}{436}$ $\frac{437}{438}$ $\frac{439}{440}$ $\frac{441}{442}$ $\frac{443}{444}$ $\frac{445}{446}$ $\frac{447}{448}$ $\frac{449}{450}$ $\frac{451}{452}$ $\frac{453}{454}$ $\frac{455}{456}$ $\frac{457}{458}$ $\frac{459}{460}$ $\frac{461}{462}$ $\frac{463}{464}$ $\frac{465}{466}$ $\frac{467}{468}$ $\frac{469}{470}$ $\frac{471}{472}$ $\frac{473}{474}$ $\frac{475}{476}$ $\frac{477}{478}$ $\frac{479}{480}$ $\frac{481}{482}$ $\frac{483}{484}$ $\frac{485}{486}$ $\frac{487}{488}$ $\frac{489}{490}$ $\frac{491}{492}$ $\frac{493}{494}$ $\frac{495}{496}$ $\frac{497}{498}$ $\frac{499}{500}$ $\frac{501}{502}$ $\frac{503}{504}$ $\frac{505}{506}$ $\frac{507}{508}$ $\frac{509}{510}$ $\frac{511}{512}$ $\frac{513}{514}$ $\frac{515}{516}$ $\frac{517}{518}$ $\frac{519}{520}$ $\frac{521}{522}$ $\frac{523}{524}$ $\frac{525}{526}$ $\frac{527}{528}$ $\frac{529}{530}$ $\frac{531}{532}$ $\frac{533}{534}$ $\frac{535}{536}$ $\frac{537}{538}$ $\frac{539}{540}$ $\frac{541}{542}$ $\frac{543}{544}$ $\frac{545}{546}$ $\frac{547}{548}$ $\frac{549}{550}$ $\frac{551}{552}$ $\frac{553}{554}$ $\frac{555}{55$



Protections Implemented by Browsers

IE (9) shows Punycode if

- ▣ If there is a mismatch between the characters used in the URL and the language expectation

This web address contains letters or symbols that can't be displayed.

[Change language settings](#)

[Don't show this message again](#)



- ▣ If character is not used in any language
- ▣ Mixed set of scripts that do not belong



Protections Implemented by Browsers

Chrome (18.0.1025.142) shows Punycode if

- ▣ Configured language of the browser (configured in the “Fonts and Languages” options) does not match
- ▣ Incompatible set of scripts that do not belong
 - But there is a whitelist, so hard to confuse scripts like Latin with Chinese can be used
- ▣ Characters in a black list



Defenses by Registrar

- ▣ Registrars may not allow the character
- ▣ For example, one registrar gave the following error when an attempt was made to register iucu.org (Cyrillic small letter Byelorussian-Ukrainian i U+0456):
“Error: You used an invalid international character! Please note that for some reason .org and .info only support Danish, German, Hungarian, Icelandic, Korean, Latvian, Lithuanian, Polish, Spanish, and Swedish international characters.”
- ▣ May be gotten around by / homoglyphs, / Katakana Letter No (U+30ce) seems to work best



Approach

1. How different browsers show the Punycode in the URL bar.
 2. How different mail systems show the URL when email is displayed.
 3. How social networks render the URL.
- ▣ Used domain we control, and Local Hosts file to map the DNS entries

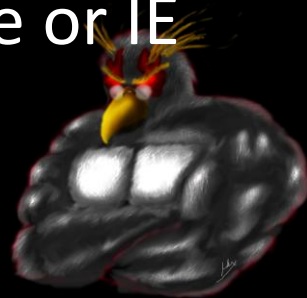


Some Results

URL	Firefox 11	IE 9	Chrome 18.0.1025.142
U+03A9 <u>Ω.com</u>	<u>xn--bya.com</u>	<u>xn--bya.com</u>	<u>xn--bya.com</u>
Ω U+03A9 <u>Ω.org</u>	<u>Ω.org</u>	<u>xn--exa.org</u>	<u>xn--exa.org</u>
g U+0261 <u>google.com</u>	<u>xn--oogle-qmc.com</u>	<u>xn--oogle-qmc.com</u>	<u>xn--oogle-qmc.com</u>
i U+0456 <u>iucu.org</u>	<u>iucu.org</u>	<u>xn--ucU+ihd.org</u>	<u>xn--ucU+ihd.org</u>
g U+FF47 o U+FF4F o U+FF4F g U+FF47 l U+FF4C e U+FF45 g o o g l e .com	Normalized to standard Latin	Normalized to standard Latin	Normalized to standard Latin
/ U+204 <u>www.microsoft.com/in dex.html.irongeek.org</u>	<u>www.microsoft.xn-- comindex- g03d.html.irongeek.org</u>	<u>www.microsoft.xn-- comindex- g03d.html.irongeek.org</u>	<u>www.microsoft.xn-- comindex- g03d.html.irongeek.org</u>

Other odd balls

- ▣ iucu.org (i U+0456) could not be registered
- ▣ These seemed to pass Registrar's tests
 - íucu.org [xn--ucU+2ia.org](Latin capital letter i with acute í U+0456)
 - íucu.org [xn--ucU+qma.org](Latin small letter i with acute í U+00ED)
 - jucu.org [xn--ucU+9ta.org](Latin small letter i with ogonek j U+00ED)
- ▣ ノ Katakana Letter No (U+30ce) seems to work in Firefox for subdomain trick, but not in Chrome or IE



Display of IDNA in Web Apps

- ▣ What does the webapp display?
- ▣ How does it parse links?



Test Strings

Ω U+03A9

<http://Ω.com>

g U+0261

<http://google.com>

<http://google.org>

i U+0456

iucu.org

<http://iucu.org>

/ U+2044

<http://www.microsoft.com/index.html.irongeek.com>

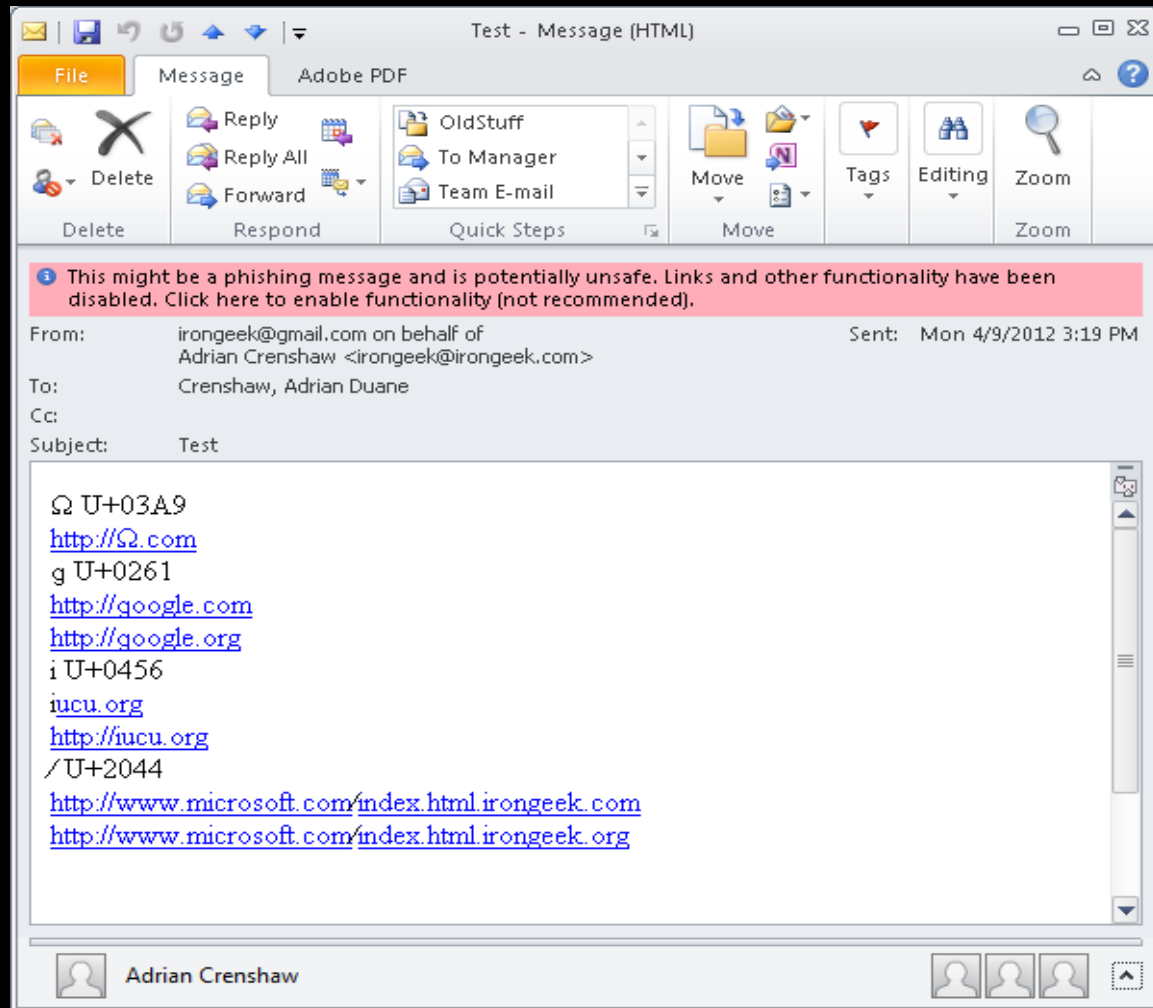
<http://www.microsoft.com/index.html.irongeek.org>

<http://Irongeek.com>



Outlook 2010

- ▣ Sent from Gmail to campus mail
- ▣ Pink phishing warning that must be clicked past to use links
- ▣ 4th, 7th and 8th link had parse errors



File

Message

Adobe PDF

Delete

Reply

Reply All

Forward

Respond

OldStuff

To Manager

Team E-mail

Quick Steps

Move

Move

Tags

Tags

Editing

Editing

Zoom

Zoom

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: irongeek@gmail.com on behalf of Adrian Crenshaw <irongeek@irongeek.com> Sent: Mon 4/9/2012 3:19 PM

To: Crenshaw, Adrian Duane

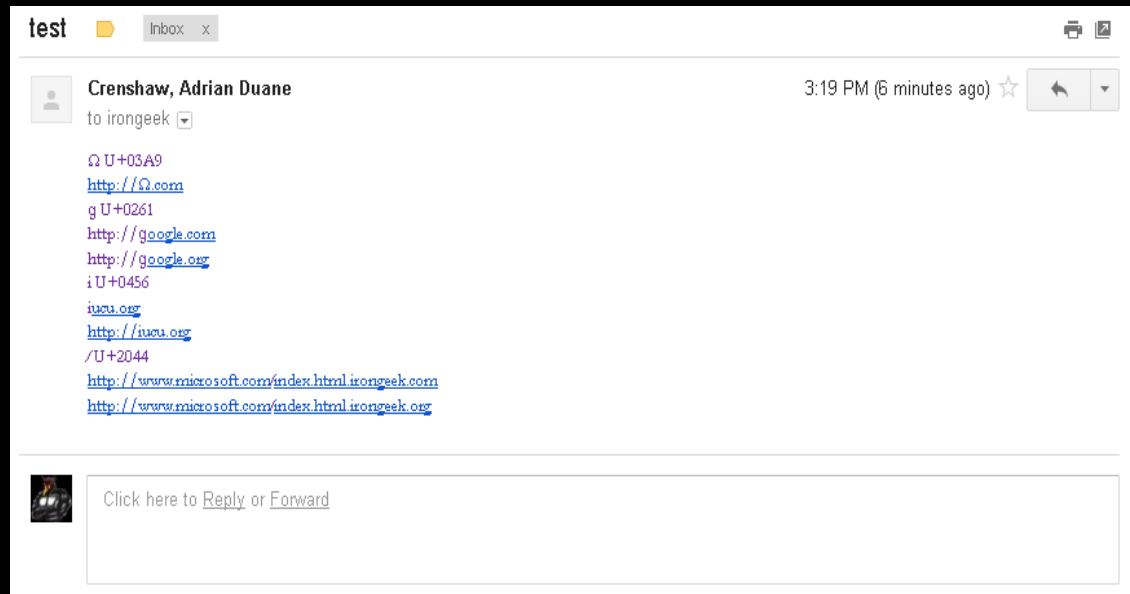
Cc:

Subject: Test

Ω U+03A9
<http://Ω.com>
 g U+0261
<http://google.com>
<http://google.org>
 i U+0456
<http://iucu.org>
<http://iucu.org>
 /U+2044
<http://www.microsoft.com/index.html.irongeek.com>
<http://www.microsoft.com/index.html.irongeek.org>

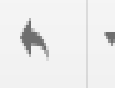
Gmail

- ❑ Sent from campus mail to Gmail
- ❑ 2nd and 3rd links had problem with g (Latin small letter script G U+0261)
- ❑ 4th link had problems with Cyrillic i (U+0456) if no http:// in front
- ❑ 7th and 8th link had parse errors because of / (fraction slash U+2044) and were split in two



**Crenshaw, Adrian Duane**

3:19 PM (6 minutes ago) ☆



to irongeek ▾

Ω U+03A9

<http://Ω.com>

g U+0261

<http://google.com><http://google.org>

i U+0456

iuua.org<http://iuua.org>

/U+2044

<http://www.microsoft.com/index.html.irongeek.com><http://www.microsoft.com/index.html.irongeek.org>Click here to [Reply](#) or [Forward](#)

Facebook

- Seemed to render all but the fourth link as it was inputted
Punycode versions show
- iucu.org without the preceding http:// gave issues. Cyrillic i (U+0456) seemed to confuse the parser
- The / (fraction slash U+2044) in the last two links seems to also cause no oddities



Adrian Crenshaw

Ω U+03A9

<http://Ω.com/>

g U+0261

<http://google.com/>

<http://google.org/>

i U+0456

iucu.org

<http://iucu.org/>

/ U+2044

<http://www.microsoft.com/index.html.irongeek.com/>

<http://www.microsoft.com/index.html.irongeek.org/>



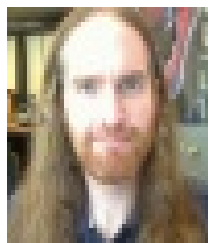
Future Home of The Omega Project

www.xn--bya.com

"A lot of outstanding guys figure they'll pledge Omega, or they won't pledge at all" -- Greg Marmalard (Faber College, Class of '64)

Like · Comment · Share · a few seconds ago





Adrian Crenshaw

Ω U+03A9

<http://Ω.com/>

g U+0261

<http://google.com/>

<http://google.org/>

i U+0456

iucu.org

<http://iucu.org/>

/ U+2044

<http://www.microsoft.com/index.html.irongeek.com/>

<http://www.microsoft.com/index.html.irongeek.org/>

Ω.com

Future Home of The Omega Project

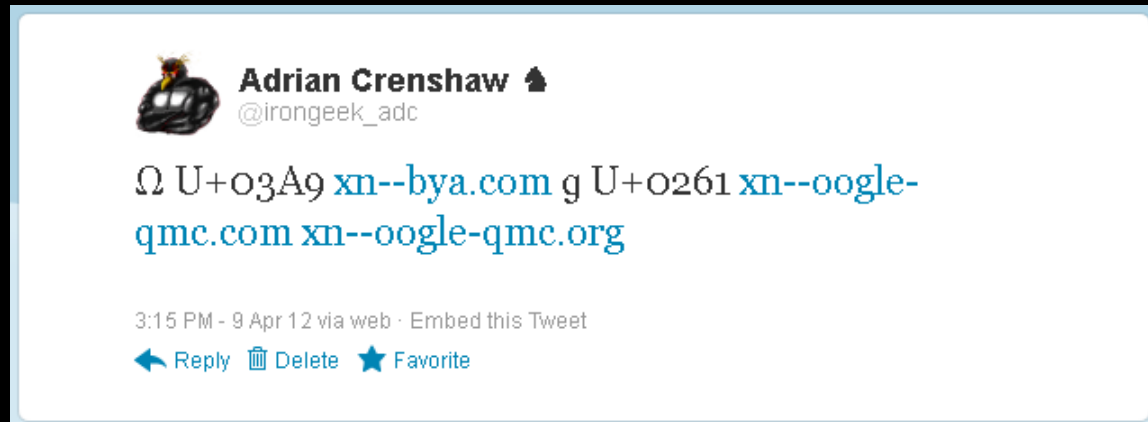
www.xn--bya.com

"A lot of outstanding guys figure they'll pledge Omega, or they won't pledge at all" -- Greg Marmalard (Faber College, Class of '64)

Like · Comment · Share · a few seconds ago

Twitter

- ❑ Twitter had the effect of rendering all of the URLs as a truncated, URL shortened (using t.co), Punycode version
- ❑ except the iucu.org without the preceding http://. Again, the soft-dotted Cyrillic i (U+0456) seemed to confuse the parser.
- ❑ Twitter makes it pretty obvious that there is something funny about the URLs





Adrian Crenshaw 🦅

@irongeek_adc

Ω U+03A9 [xn--bya.com](#) g U+0261 [xn--oogle-qmc.com](#) [xn--oogle-qmc.org](#)

3:15 PM - 9 Apr 12 via web · Embed this Tweet

← Reply 🗑 Delete ★ Favorite



Adrian Crenshaw 🦅

@irongeek_adc

i U+0456 [iucu.org](#) [xn--ucu-ihd.org/U+2044](#)
[...t.xn--comindex-go3d.html.irongeek.com](#) [...t.xn--comindex-go3d.html.irongeek.org](#)

3:15 PM - 9 Apr 12 via web · Embed this Tweet

← Reply 🗑 Delete ★ Favorite

MORE IDEAS?



Canonicalization Errors?

- ▣ Remember when the full width Latin forms were turned to normal latin in the URL bar?
- ▣ < or > filtered?
- ▣ What if it also tries to canonicalize similar characters like < (U+003c), >(U+003e), ‹ (U+2039), › (U+203a), ‹(U+ff1c), ›(U+ff1e) afterwards?



Name Spoofing

- ▣ IP Boards let me spoof Daren from Hak5's screen name: Darren Kitchen (U+039A Greek Capital Letter Kappa)
vs
Darren Kitchen
- ▣ Twitter returned the error
"Invalid username! Alphanumerics only."
- ▣ Gmail/Google returned the error
"Please use only letters (a-z), numbers, and periods." when non-ASCII characters were attempted.
- ▣ Windows 7 let me use Unicode
- ▣ OS X Lion seems to replace or remove the characters
- ▣ More research needs to be done in these areas.



Right to left?

- ▣ Josh Kelley mentioned this one to me
- ▣ What about left to right mixed with right to left scripts?
- ▣ Takes U+202E (Right-to-Left Override)
- ▣ <http://irongeek.com>
- ▣ <http://irongeek.com/moc.tfosorcim//:ptth>
- ▣ More details at:
<http://digitalpbk.blogspot.com/2006/11/fun-with-unicode-and-mirroring.html>



What about file names?

- ▣ txt.bat
- ▣ txt.vbs
- ▣ txt.exe
- ▣ txt.com
- ▣ txt.docx

Demo



Just how they are displayed

```
C:\Users\adrian\Desktop\examples>dir
Volume in drive C is BOOTCAMP
Volume Serial Number is 0462-A90F
```

Directory of C:\Users\adrian\Desktop\examples

```
05/16/2012  11:44 AM  <DIR>          .
05/16/2012  11:44 AM  <DIR>          ..
05/16/2012  11:43 AM                273 test.au3
05/16/2012  11:24 AM                69 wickednames.txt
05/16/2012  11:30 AM                39 ?txt.bat
05/16/2012  11:31 AM            12,551 ?txt.docx
05/16/2012  11:43 AM           302,117 ?txt.exe
05/16/2012  11:28 AM                24 ?txt.vbs
        6 File(s)        315,073 bytes
        2 Dir(s)  19,766,902,784 bytes free
```

```
C:\Users\adrian\Desktop\examples>
```



Useful Sites

- ▣ Unicode Security Considerations
<http://unicode.org/reports/tr36/>
- ▣ Unicode Converter
<http://www.rishida.net/tools/conversion/>
- ▣ Unicode Character Info and List
<http://www.fileformat.info/>
- ▣ Homoglyph Attack
Generator<http://www.irongeek.com/homoglyph-attack-generator.php>



References

- ▣ A. Costello, March 2003. [Online]. Available: <http://www.ietf.org/rfc/rfc3492.txt>.
- ▣ J. Abolins, December 2010. [Online]. Available: <http://www.irongeek.com/i.php?page=videos/dojocon-2010-videos#Internationalized%20Domain%20Names%20&%20Investigations%20in%20the%20Networked%20World>.
- ▣ M. Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, 1st ed., No Starch Press, 2011.
- ▣ E. & G. A. Gabrilovich, "The Homograph Attack," Communications of the ACM , vol. 45, no. 2, 2002.
- ▣ V. Krammer, "Phishing defense against IDN address spoofing attacks," in Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services , New York, NY, USA, 2006.
- ▣ E. Johanson, "The state of homograph attacks," 2005. [Online]. Available: <http://www.shmoo.com/idn/>. [Accessed 24 4 2012].
- ▣ D. Kennedy. [Online]. Available: <http://www.secmaniac.com/download/>.
- ▣ A. Crenshaw, 2012. [Online]. Available: <http://www.irongeek.com/homoglyph-attack-generator.php>.
- ▣ phlyLabs, 2012. [Online]. Available: <http://phlymail.com>.
- ▣ Microsoft, September 2006. [Online]. Available: <http://msdn.microsoft.com/en-us/library/bb250505%28VS.85%29.aspx>.
- ▣ Chromium Project, [Online]. Available: <http://www.chromium.org/developers/design-documents/idn-in-google-chrome>.
- ▣ C. Weber, July 2009. [Online]. Available: <http://www.blackhat.com/presentations/bh-usa-09/WEBER/BHUSA09-Weber-UnicodeSecurityPreview-SLIDES.pdf>.
- ▣ C. Weber, July 2009. [Online]. Available: <http://www.blackhat.com/presentations/bh-usa-09/WEBER/BHUSA09-Weber-UnicodeSecurityPreview-PAPER.pdf>.
- ▣ A. Crenshaw, "Steganographic Command and Control: Building a communication channel that withstands hostile scrutiny," 2010. [Online]. Available: <http://www.irongeek.com/i.php?page=security/steganographic-command-and-control>. [Accessed 23rd April 2012].



Events



Sept 27th-30th 2012

<http://www.derbycon.com>

Derbycon Art Credits to Digip



Photo Credits to KC (devauto)

Others

<http://www.louisvilleinfosec.com>

<http://skydogcon.com>

<http://hack3rcon.org>

<http://outerz0ne.org>

<http://phreaknic.info>

<http://notacon.org>



<http://lrongeek.com>

QUESTIONS?

42

Twitter: @Irongeek_ADC



- ▣ [http://www.microsoft.com/](http://www.microsoft.com/index.html)[index.html.irongeek.org/](http://www.irongeek.org/)
- ▣ <http://www.microsoft.xn--comindex-634g.html>[irongeek.org/](http://www.irongeek.org/)

