JASK

THREAT ADVISORY

Domain Hijacking/ Impersonation Attack Campaigns

AUTHOR
ROD SOTO

JASKLABS
TA-0007

TLP
WHITE

RISK FACTOR
HIGH

THREAT ADVISORY

Domain Hijacking/Impersonation Attack Campaigns

AUTHOR
ROD SOTO

JASKLABS
TA-0007

TLP
WHITE

RISK FACTOR
HIGH

Overview

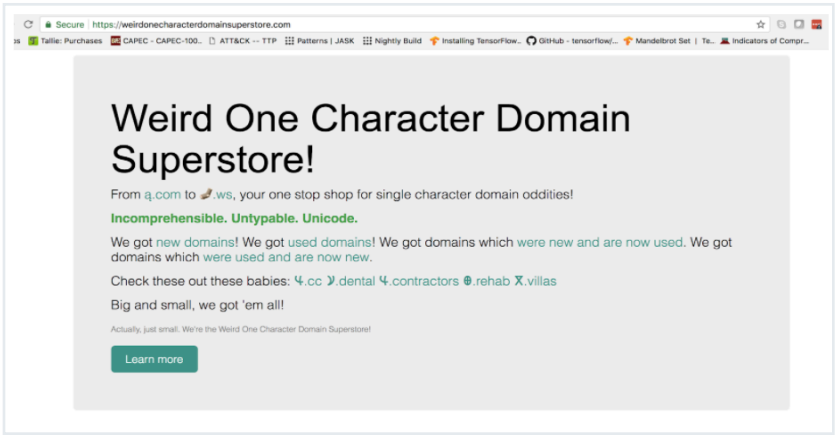
Recent malicious campaigns demonstrate the targeting of an organization's internet domain in order to take control of its resources and customer data. This technique, known as domain hijacking, allows malicious actors to acquire the internet domain of an organization and proceed to take over all of its resources and operations. Once the domain has been obtained, malicious actors proceed to impersonate victims and interact with assets, customers and any resource that can be obtained through impersonation of the internet domain. A new type of impersonation has been reported recently by the use of "Punycode." "Punycode" is a way to represent International Domain Names (IDNs) with the limited character set (A-Z, 0-9) supported by the domain name system."*

In many instances the use of Punycode can go unnoticed by standard users who do not realize that what is presented in the browser address bar is the result of a translation from an international domain name that has nothing to do with the actual site they are trying to access, but looks exactly like it when translated into the browser bar. This allows attackers to register a punycode domain clone, target a domain site, get an actual SSL certificate and then proceed to expose it to potential victims.

Indicators

In order to successfully impersonate or hijack an internet domain, malicious actors must devise a punycode or a special character that is able to translate into the desired domain to impersonate. There are many tools available on the internet that allow malicious actors to "translate" such a character into a targeted domain, or simply create a subdomain with URLs that contain a minor and often-overlooked typo, such as Goooogle.com or Amazoon.com.

Fig 1 Shows store for non standard character domains



AUTHOR
ROD SOTO

JASKLABS
TA-0007

TLP
WHITE

RISK FACTOR
HIGH

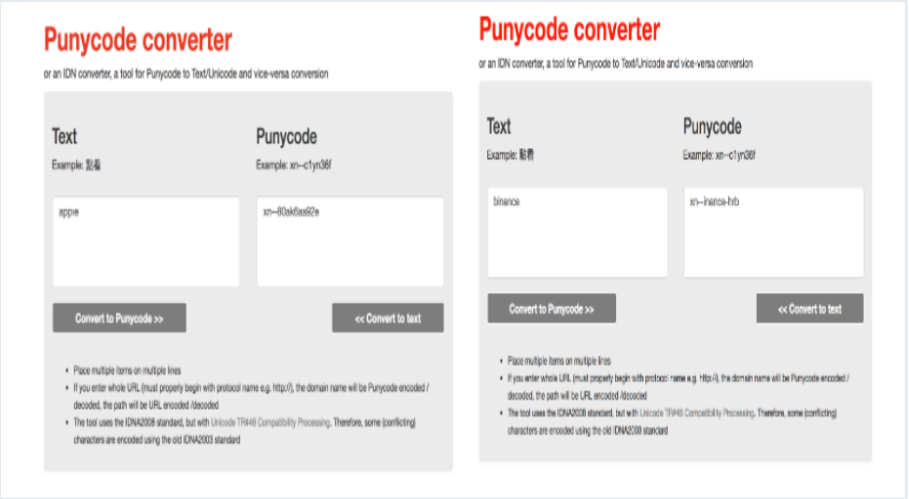
Human perception and gullibility play a big role in these types of attacks. It is important to point out that a simple mouse-over in desktop-type systems may in some cases allow a victim to discover the real domain. This is not possible in other types of devices such as phones, which makes this attack more likely to succeed.

Once attackers are able to successfully mislead victims, they can then escalate to many other types of malicious attack vectors, such as pushing malware, grabbing credentials, pivot from current sessions into cloned websites, and escalate even further as victims interact with them as a trusted entity.

Lab Study / Case Study

The following field/laboratory study shows a couple of cases where malicious actors were able to find IDNs, that once translated into ASCII present the victim domain names that impersonate other reputable and known internet domains. The goal is to obtain an IDN that once translated to ASCII will match the desired targeted organization. The following graphic shows an online punycode converter and two examples of IDNs that once translated match known organizations that posses such domain in ASCII characters.

Fig 2 Shows how a punycode set of characters can be translated as a known word in browser



Once the punycode matching code is found, malicious actors can proceed to register such a domain, preferably on foreign registrars. There have been many instances of foreign registrars where, due to international jurisdiction and lack of security, massive theft of domains have occured.

It is also very likely that jurisdictions with lack of regulations and supervision from central registrars would allow creation and registration of IDNs that would match well-known internet domains when translated into ASCII. This pretty much allows malicious actors to hijack a domain without the need to actually compromise the real one.

AUTHOR
ROD SOTO

JASKLABS
TA-0007

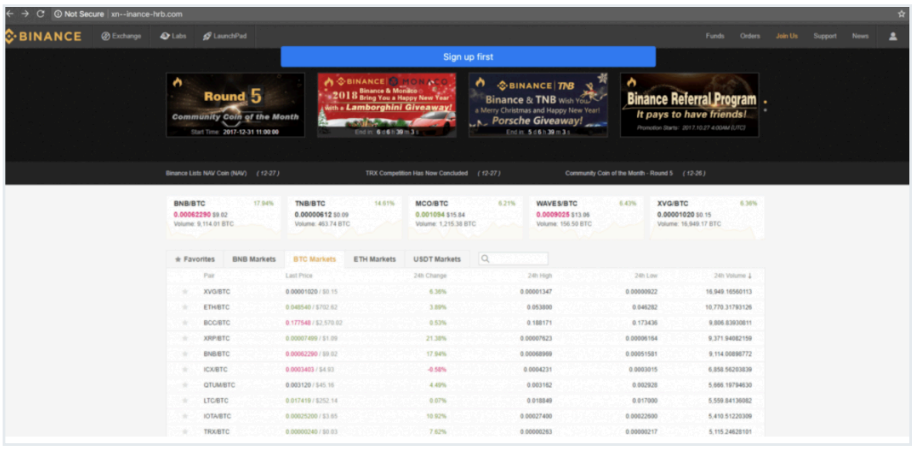
TLP
WHITE

RISK FACTOR
HIGH

As stated above, malicious actors also can try non-standard characters and create subdomains of targeted organizations, looking less suspicious than typo squads or other types of domain character creation techniques that appear close to the original in order to facilitate phishing.

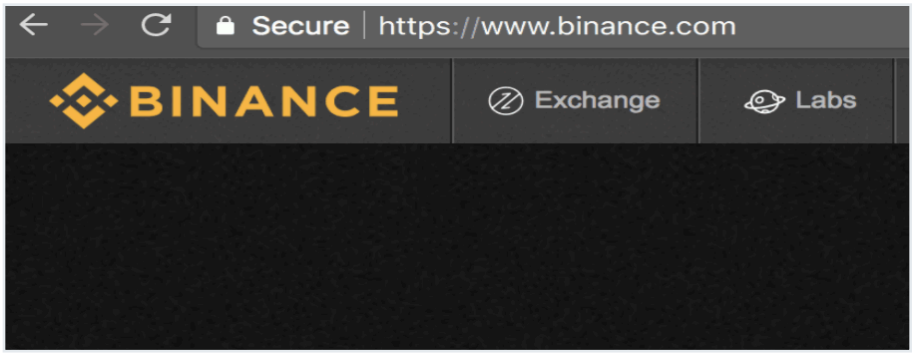
The following graphic taken from a NextWeb article shows a recent malicious campaign where a cryptocurrency exchange site was targeted. Malicious actors registered punycode domain xn-inance-hrb.com (Translates above as binance) then proceeded to get SSL certificates, clone the actual real site then present the site via multiple means (forums, social media, emails, chats, etc).

Fig 3 Shows recent impersonation of a Cryptocurrency exchange site Binance *



The image above and the next one below show how effective and difficult to detect this type of attack can be. Any standard user would not have been able to catch this site as an impersonator. Furthermore, the image below shows a standard icon for a secure genuine site which is usually one of the things users are told to check for.

Fig 4 Shows browser lock icon showing site is apparently genuine and secure *



AUTHOR
ROD SOTO

JASKLABS
TA-0007

TLP
WHITE

RISK FACTOR

HIGH

Mitigation

Although these type of attacks are very difficult to detect by standard users, and even though this is not a direct compromise of an actual internet domain, there are measures that can be taken in order to protect against these types of attacks.

- Protect your domain registrars accounts so they cannot be compromised and your domain redirected. (Multiple Factor Authentication, Complex Passwords, Private Registrations)
- Select reputable domain registrars that will have support and legal weight in case of domain misappropriation/dispute.
- Monitor for impersonation and registration of rogue/non-standard character domains that may be used against your organization.
- Use tools such as Domain Lock (prevent transfer). DNSSEC (DNS secure verification of actual domain and name servers) can help users to detect impersonating sites and deter malicious actors.
- Properly document your domain. It is not far fetched that malicious actors can at one point attempt to claim ownership based on previous registration or other geopolitical factors.
- Utilize web filters and blacklists to help prevent some of these attacks.

For Users

- Do not install mobile applications outside of authorized application stores.
- Install punycode alert add-ons from internet browsers authorized stores.
- Train users in security awareness of these types of attacks.
- Do not open or click on hyperlinks sent by strangers or unexpected from known entities.