MS-ISAC®

MS-ISAC Security Primer

Typosquatting

February 2018, SP2018-0108

Typosquatting attempts to take advantage of typographical errors (i.e. "typos") introduced by users when URLs are typed directly into the address bar. By capitalizing on user error, cyber threat actors funnel unsuspecting users to illegitimate domains that closely mimic originals. This tactic involves the purchase and registration of domains similar to an existing domain. Typosquatters often target high-traffic and/or sensitive websites to exploit the greatest number of users or to gain unauthorized access to restricted information. These domains are visually similar to the original, increasing the likelihood of successful attack. Cyber threat actors create similar websites by scraping the HTML from legitimate websites and replicating it on typosquatted domains with minor malicious changes. Successful cases of typosquatting are used to generate ad revenue, display custom images or text, further scams and frauds, capture login credentials, and/or infect users with malware.

There are six main variations of typosquatting. A typosquatted domain may contain one or several of these variations to deceive users. The following examples are based on the *cisecurity.org* domain.

1. Omission – characters are removed
   - "csecurity[.]org" *(the first "**i**" has been omitted)*
2. Addition – characters are added
   - "cissecurity[.]org" *(an "**s**" has been added)*
3. Substitution – characters are swapped
   - "cisecurlty[.]com" *(last "**i**" and "**.org**" swapped for "**l**" and "**.com**")*
4. Transposition – characters are relocated
   - "csiecurity[.]org" *(the first "**i**" switched places with "**s**")*
5. Hyphenation – domain portion(s) are hyphenated
   - "ci-security[.]org" *(hyphen added between "**i**" and "**s**")*
6. Homoglyph – character homographs (lookalikes) used
   - "cisecurity[.]org" *(first Latin "**i**" and "**y**" homographed with Cyrillic character "U" that looks like a Latin "**y**" and Cyrillic character "Dotted I" that looks like a Latin "**i**")*

***Domain Name Scam*:** *In this scam, a Chinese domain name registration company attempts to take advantage of substitution typosquatting by sending a letter or email that a company is trying to register your domain. The company claims to be giving you the opportunity to protect your domain by buying it with alternate top level domains (e.g. .cc, .cn, .net etc.). The scam is that no one is trying to register your domain and the company is charging significantly higher than normal domain registration fees.*

USER RECOMMENDATIONS:

- When visiting known websites, ensure the URL is free from typographical errors. If the URL is not known, use an Internet search engine to identify the legitimate website.
- Verify links before clicking on them. The easiest way to check a link is by hovering over it with your mouse and carefully checking for typosquatting techniques; bookmark websites you visit often.

TECHNICAL RECOMMENDATIONS:

- Use WHOIS lookups and/or other web reputation tools to verify the legitimacy of domains.
- Run dnstwist services against domains you own to see if they are actively being typosquatted.
- Run an Internet query for terms associated with your domain to ensure it is the first result.
- Consider purchasing variations of your domains to protect against common typographical errors.
- If one of your domains is typosquatted, consult ICANN for inquiries into filing a Uniform Domain Name Dispute Resolution Policy (UDRP) and review other available actions under the United States' Anticybersquatting Consumer Protection Act (ACPA).

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/.