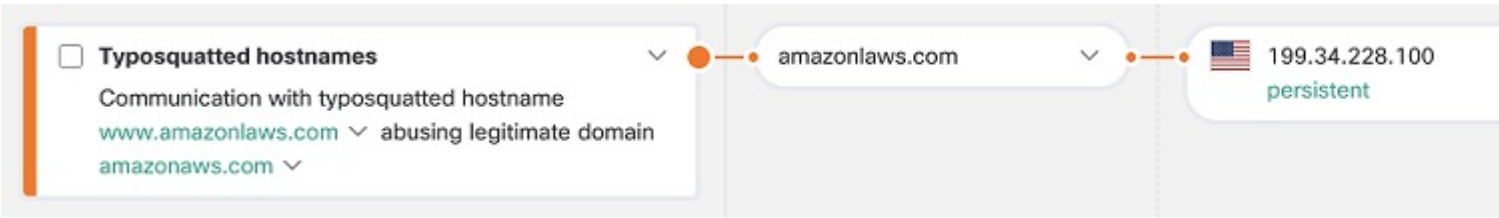
March 2021

Updates released in March of 2021 to Cisco cloud-based machine learning global threat alerts:

New Typosquatting Classifier

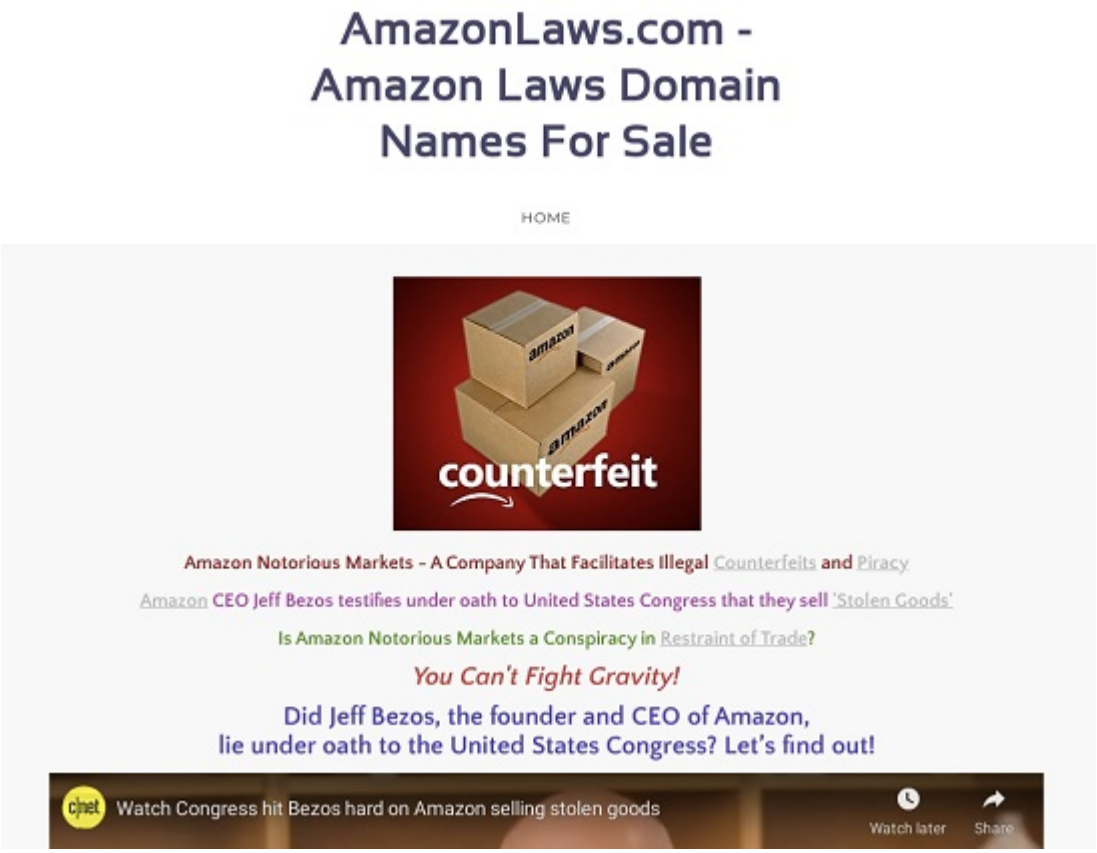
Typosquatting is a form of URL hijacking that relies on typographical errors (typos) made by users while entering a URL into their web browser. This results in the user being directed to an alternative website owned by an attacker. The typosquatting URL is visually similar to the legitimate URL, such as:

Figure 1: Example: typosquatted hostname which has an extra letter added



The typosquatting URL usually directs to online scams, such as advertising pages used to generate profit from ads or phishing pages used to steal information from users.

Figure 2: Example: advertising page targeting users intending to go to Amazon AWS



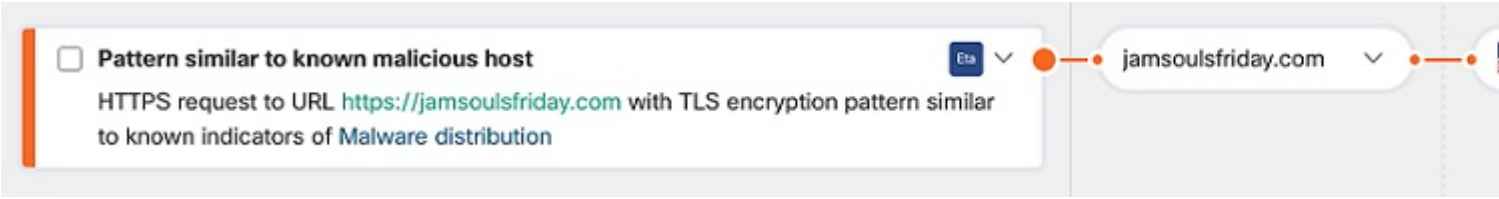
The new classifier aims to protect users from typosquatting domains targeting most popular domains. The classifier effectively identifies the domains similar to the most popular domains by calculating the similarity of domains. The classifier then determines the severity of the threat based on additional parameters, such as the age of the typosquatting domain.

This can be seen in **Alert** > **Alert detail** > **Security events**.

New TLS Pattern Classifier

The new classifier is built on top of Transport Layer Security (TLS) fingerprinting technologies. Taking into account TLS headers from Encrypted Traffic Analytics (ETA) and additional global and local context features, the classifiers detects suspicious and malicious applications based on their TLS footprint. Through analysis of encrypted communication, the classifier extends the capabilities of models aimed at threats communicating by HTTP.

Figure 3: Example: TLS pattern similar to a host known to be malicious



This can be seen in **Alert** > **Alert detail** > **Security events**.