From: Kaliski, Burt
Sent: Friday, November 15, 2013 1:30 PM
To: Akram Atallah; John L. Crain

Subject: Verisign Labs continued analysis of SLD blocking effectiveness

Dear Messrs. Atallah and Crain,

Last week, I shared a preliminary analysis performed by Verisign Labs of the queries seen at the A and J root servers for the nine gTLDs whose SLD blocking lists were published on October 29. Our initial results indicated that a significant number of potentially at-risk queries would remain even if SLD blocking is implemented.

Verisign Labs has continued that analysis and confirmed that similar findings apply to the batch of 16 gTLDs whose SLD blocking lists were published on November 6.

Our research also continues to confirm that a snapshot of past queries such as the DITL data is not a reliable predictor of future activity. This point can even be verified by analyzing the DITL data itself, without reference to external data sets, as the attached Verisign Labs note illustrates.

Please let me know if you have any questions.

Sincerely,

Burt

Burt Kaliski Jr. Senior Vice President and CTObkaliski@Verisign.comm: 571-528-2679 t: 703-948-4664
12061 Bluemont Way, Reston, VA 20190VerisignInc.com

Continued Analysis of SLD Blocking Effectiveness

Verisign Labs
November 15, 2013

Verisign Labs recently did a preliminary analysis of the queries seen at the A and J root servers, which Verisign operates, for the nine gTLDs whose SLD blocking lists were published on October 29. Verisign Labs' analysis of these gTLDs, reported on November 5[1], indicated, as anticipated, that installed systems are sending many queries to the root server system that include SLDs not on the blocking lists. Verisign Labs has subsequently made similar findings on the batch of 16 gTLDs whose SLD blocking lists were published on November 6. These results are a continuation of the research that Verisign Labs published earlier this year in two technical reports[2] [3].

A fundamental reason that SLD blocking based on DITL datasets is ineffective is that the set of SLDs in queries *evolves*. New SLDs appear in queries all the time. As a result, the snapshot of past queries reflected in the DITL datasets is not a reliable predictor of future activity.

The DITL data itself shows this to be the case. In particular, Verisign Labs' analysis of the DITL data shows that **the number of SLDs observed in the DITL data for the first time each year is on a significant upward trend.** Verisign Labs analyzed the root server data in the DITL datasets as follows:

- All applied-for gTLDs were included, except for those for .CORP and .HOME, which have a very high transaction volume
- Invalid domain names and the so-called Chrome-10 strings were excluded

The number of SLDs observed for the first time in a given year's DITL dataset was then recorded.

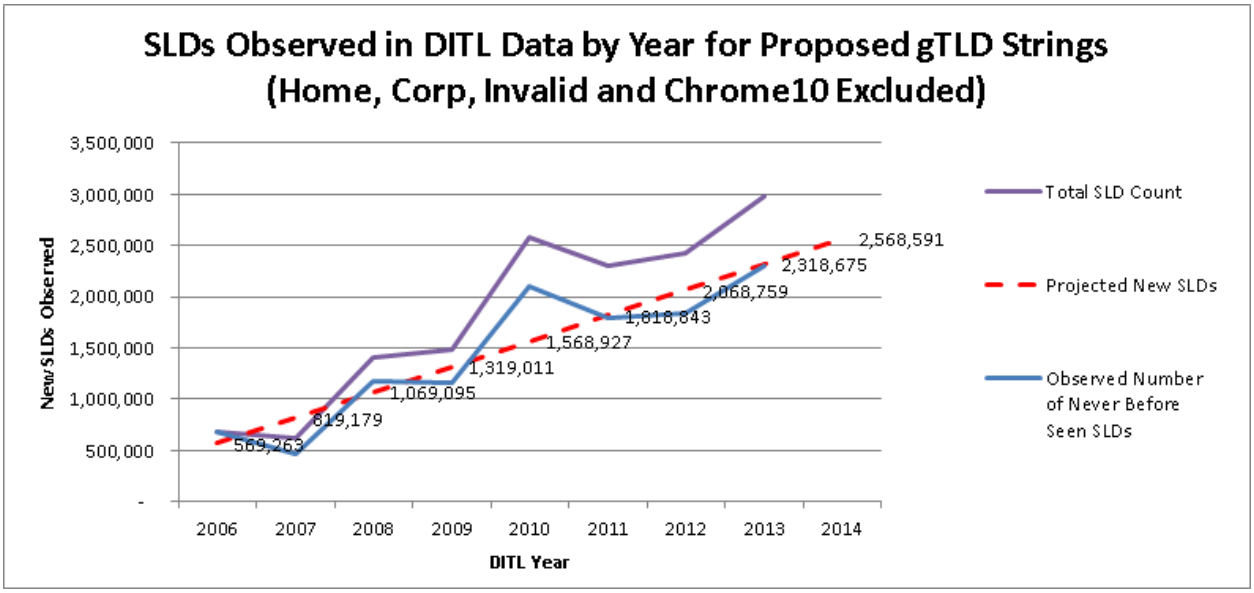
In the 2013 DITL dataset alone, there were about 2.3 million first-time SLDs across these gTLDs, out of a total observation of 3.0 million. Based on a linear best-fit, there would be another 2.6 million first-time SLDs in the 2014 dataset. Each of these presents an opportunity for at-risk queries that would not be mitigated by SLD blocking. Because the most recent DITL data collection was in May 2013, many of these anticipated first-time SLDs are likely already appearing in queries today. Other SLDs might not be seen in the next DITL dataset at all, depending on how frequently they are queried across the root server system, and how many root servers are involved in the data collection. This is another motivation for further research.

---

[1] *Preliminary Analysis of SLD Blocking Effectiveness.* Verisign Labs, November 5, 2013. Included as attachment in Letter from B. Kaliski to A. Atallah and J.L. Crain, November 5, 2013.

[2] *New gTLD Security and Stability Considerations*. Verisign Labs Technical Report #1130007. Version 2.2, March 28, 2013.

[3] *New gTLD Security, Stability, Resiliency Update: Exploratory Consumer Impact Analysis*. Verisign Labs Technical Report #1130008. Version 1.1, August 27, 2013.


SLDs Observed in DITL Data by Year for Proposed gTLD Strings
(Home, Corp, Invalid and Chrome10 Excluded)
New SLDs Observed
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
-
2006
2007
2008
2009
2010
2011
2012
2013
2014
DITL Year
569,263
819,179
1,069,095
1,319,011
1,568,927
1,818,843
2,068,759
2,318,675
2,568,591
Total SLD Count
Projected New SLDs
Observed Number of Never Before Seen SLDs