From: Kaliski, Burt
Sent: Tuesday, November 05, 2013 5:23 PM
To: Akram Atallah; John L. Crain

Subject: Verisign Labs preliminary analysis of SLD blocking effectiveness

Dear Messrs. Atallah and Crain,

Verisign Labs recently performed 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.   Our initial results, which we are sharing in the interest of timeliness, indicate that a significant number of potentially at-risk queries would remain even if SLD blocking is implemented. The attached note summarizes these findings.

We encourage ICANN to review the process by which the SLD blocking lists were constructed that resulted in the omission of the SLDs associated with the potentially at-risk queries. It is unclear to us how the lists were constructed, including which particular DITL data sets were employed per ICANN's October 4 New gTLD Collision Occurrence Management Proposal. Moreover, it is not clear what outreach is planned to operators of installed systems potentially impacted by the nine gTLDs. We also repeat our recommendation, given in prior communications to ICANN, to move toward a more qualitative approach to risk mitigation.

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

This message (including any attachments) is intended only for the use of the individual or entity to which it is addressed, and may contain information that is non-public, proprietary, privileged, confidential and exempt from disclosure under applicable law or may be constituted as attorney work product. If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this message in error, notify sender immediately and delete this message immediately.

Preliminary Analysis of SLD Blocking Effectiveness

Verisign Labs
November 5, 2013

As part of Verisign's ongoing commitment to security, stability and resiliency of the Domain Name System, Verisign Labs has been continuing the research it published earlier this year in two technical reports[1] [2]. Verisign Labs recently did a preliminary analysis of the queries seen at the A and J root servers, which Verisign operates, for the gTLDs whose SLD blocking lists were published on October 29:

.camera, .clothing, .equipment, .guru, .holdings, .lighting, .singles, .ventures, .voyage

Verisign Labs' analysis indicates, as anticipated, that installed systems are sending many queries to the root server system that include SLDs not on the blocking lists.

This note calls out one example for immediate attention.

In the second technical report, Verisign Labs identified the WPAD and ISATAP query types as potential risk vectors. These are not the only types of queries that could put an installed system at risk if the behavior of the global DNS were to change, but they are important ones because of the widespread use of the WPAD and ISATAP protocols in network configuration.

In data collected at the A- and J- root servers during a three-month period from July to October 2013, Verisign Labs observed **918 WPAD queries** and **403 ISATAP queries** from one third-level domain within the .holdings gTLD. This third-level domain was within an **SLD not on the blocking list.**

Because the SLD is not on the blocking list, it is possible that the SLD could be registered within the gTLD, changing the behavior of the global DNS for the installed system that generated these queries, with unpredictable consequences. In addition, as noted, many other SLDs not on the blocking lists occur in the queries to the root server system. Changes to the global DNS for those SLDs could likewise impact installed systems.

For reference, the traffic volume that Verisign Labs measured at the A and J root servers for .holdings is visualized below. The top line of each graph shows the total number of queries measured during the period (excluding, consistent with ICANN's approach, queries for domain names that did not consist only of alphanumeric characters and dashes, and the so-called "Chrome random strings.") The bottom line

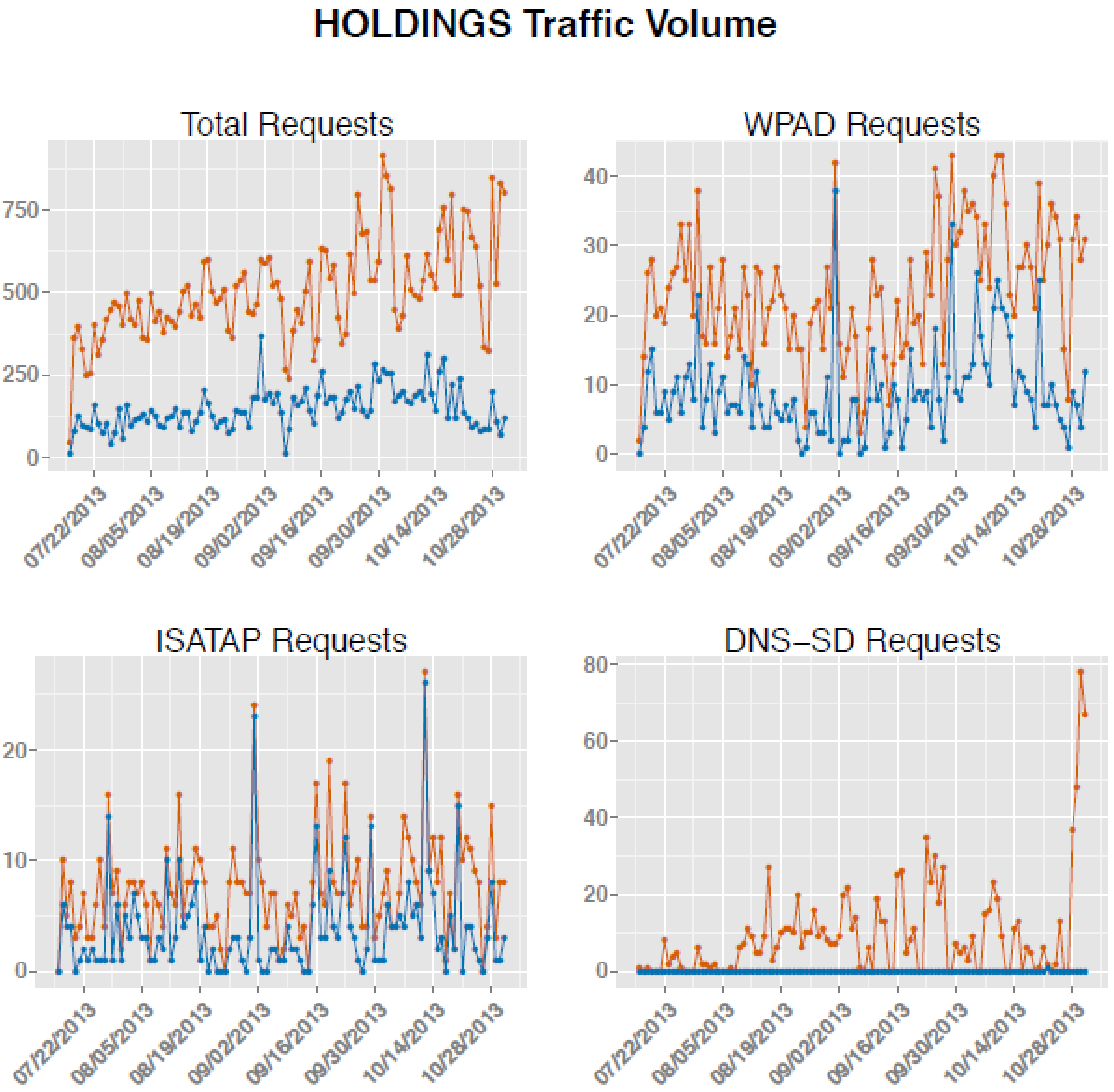
[1] *New gTLD Security and Stability Considerations*. Verisign Labs Technical Report #1130007. Version 2.2, March 28, 2013.

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

shows what the total number would have been if queries with SLDs on the blocking list were also excluded.

The SLD within .holdings mentioned above is the primary source for the unmitigated WPAD and ISATAP requests. Many other SLDs contribute to the total requests. Clearly, a significant number of potentially at-risk queries would remain if blocking were implemented.

Until more detailed analysis has been done for the queries and the installed systems that generated them, it is not possible to draw a full conclusion on the impact on installed systems if the response to those queries were to change as a result of the registration of an SLD in the new gTLDs. However, the evidence at this point underscores the argument that that the SLD blocking list is ineffective.


HOLDINGS Traffic Volume
Total Requests
WPAD Requests
ISATAP Requests
DNS–SD Requests
07/22/2013
08/05/2013
08/19/2013
09/02/2013
09/16/2013
09/30/2013
10/14/2013
10/28/2013