When Certificate Transparency Is Too Transparent

Analyzing Information Leakage in HTTPS Domain Names

Richard Roberts
ricro@cs.umd.edu
University of Maryland, College Park

Dave Levin
dml@cs.umd.edu
University of Maryland, College Park

ABSTRACT

Certificate Transparency (CT) is a recent initiative to log all publicly available certificates, thereby adding an extra layer of accountability and auditability to certificate authorities. Unbeknownst to most users and website administrators, CT logs make all data in all certificates available *publicly* and *permanently.* Although certificates are ostensibly intended to be public (after all, their main purpose is to convey an entity's public key), administrators may inadvertently include information that can be mined by anyone. For instance, CT logs contain certificates for subdomains, which naturally facilitates subdomain enumeration. This paper asks: is there other, more sensitive information included in certificates?

We identify several types of user and enterprise information embedded within the *domain names* of certificates in CT logs. We provide queries for obtaining information such as users' names, usernames, and email addresses. We also find that CT logs can leak private enterprise information, such as business relationships, user growth measurements, and the existence of internal projects prior to their public announcements. We report initial results on how often and across how many domains information is leaked. Finally, we discuss areas of future work and potential countermeasures that administrators can take.

CCS CONCEPTS

• **Security and privacy → Web protocol security**; *Privacy protections*; Pseudonymity, anonymity and untraceability.

KEYWORDS

Certificate Transparency; Information Leakage; HTTPS

ACM Reference Format:
Richard Roberts and Dave Levin. 2019. When Certificate Transparency Is Too Transparent: Analyzing Information Leakage in HTTPS Domain Names. In *18th Workshop on Privacy in the Electronic Society (WPES'19), November 11, 2019, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3338498.3358655

1 INTRODUCTION

Certificate Transparency (CT) [18, 24, 26] is a recent, successful effort to make all TLS certificates available for public audit and analysis. With CT logs and Censys [9], one can download longitudinal datasets that contain almost *all* certificates [28]. This is thought to be a powerful step forward for security, as it allows for broad measurement of the certificate ecosystem, and it allows the security community to hold certificate authorities accountable for the certificates they issue. Certificate Transparency is undeniably a wealth of information, but is all of this information intended to be made public? Is it possible that, whether through negligence or lack of knowledge, private information is leaked through CT logs?

In this paper, we investigate the nature of private information contained in—and leaked through—CT logs. Certificates are known to include some sensitive information; for instance, prior work has demonstrated that CT logs can be used to facilitate subdomain enumeration [4, 25], which may be an unavoidable consequence of the fact that certificates permit at most one wildcard in a domain. We extend these prior observations by investigating what private information about the websites' users or business relationships is leaked in certificates. We show that there is indeed private information; that it is unnecessarily leaked; and that one need look no further than certificates' domain names to find it.

We present a several search queries that can be issued against publicly available CT logs to easily extract private information about users, business relationships, and more. Our queries are designed to investigate the leakage of private *user* information, as well as private *enterprise* information. We have applied our techniques to all certificates available from Censys as of May 18, 2019, including all certificates from CT logs. Examples of domains that leak information can be found in Appendix A.

We search for private *user* information by looking for domains which include popular surnames and given names within their subdomains. In one case, we discover the names of hundreds of participants in a Multi-Level Marketing (MLM) scheme. For websites that encode user information in their subdomains, CT logs provide an easy way to *enumerate usernames and email addresses*—an important first step in account hijacking and social engineering attacks [7, 23].

When an *enterprise's* domains that it thought were internal are accessible to the public, it may leak sensitive information—for instance, by encoding sensitive information in the domain names. We demonstrate the leakage of sensitive enterprise information via CT logs by identifying an instance in which product information leaked through CT logs prior to the product's public announcement. We also show that CT logs can leak information about customer-vendor *business relationships*, and that certificate issuance *timing* can leak information about a website's user growth over time.

The impact of our work is amplified by the recent efforts to make virtually all certificates publicly available. While *security experts* have come to expect a public ledger of certificates, it is not

WPES'19, November 11, 2019, London, United Kingdom

ACM ISBN 978-1-4503-6830-8/19/11...$15.00
https://doi.org/10.1145/3338498.3358655

clear whether *administrators* who obtain certificates do. CT logs are persistent; once private information is leaked on a certificate, that information is available forever. As a result, unlike with client-authenticating certificates, *administrators may not realize that they are divulging potentially sensitive information* to the public when they obtain certificates for domains containing their users' information. We therefore believe that private information leakage within certificate datasets represents a significant ongoing potential threat; we discuss potential countermeasures in Section 5.

Prior Work CT logs have been mined for myriad information, including analyses of phishing [2, 16], violations of security best practices [12], revocation information [17], and more [25]. Scheitle et al. [25] observed that CT logs can include leaked DNS information and can be used as a mechanism for assisting in subdomain enumeration. However, to the best of our knowledge, we are the first to observe the extent to which user and enterprise information can be leaked in CT logs.

Dataset Censys gathers certificates from both CT logs and active scans of the IPv4 space [9]. VanderSloot et al. estimate this provides coverage for over 99% of observed certificates [28]. We extracted all domain names from certificates collected by Censys as of May 18, 2019, including subject names and subject alternate names. In the remainder of this paper, we show that we can query this publicly available corpus of domains for potential privacy violations.

2 USER INFORMATION LEAKAGE

2.1 Users' Names

User surnames and given names often appear in subdomains. While this can be an intentional practice to increase an individual's online exposure, other users may be unaware that their names will, through CT logs, be publicly (and permanently) associated with a particular domain.

Methodology We search subdomains in CT logs for the 10,000 most popular U.S. surnames according to the U.S. Census [27], and for one of 7,579 common male and female given names [19, 20]. We ignore names shorter than 5 characters, as they frequently appear in substrings of common words ("Li" in "online"). To discover domains that leak information about multiple users, we sort domains by how many unique surnames and given names were included as subdomains.[1] We then manually investigate the top domains to determine if the leakage of users' names is seemingly unintentional or harmful. Finally, we return to the Censys dataset and collect all subdomains for the leaky domains. This ensures that we collect the names of all users, even those with short names or names unpopular in the United States.

Multi-Level Marketing Schemes Multi-level marketing (MLM) is a sales strategy that uses non-salaried representatives who earn a commission on their sales, as well as the sales made by anyone they recruit into the program. Former participants may not want their names permanently associated with MLM, as some organizations have histories of using predatory tactics to make money from their associates [11].

Domain	Distinct Usernames	% with Name
altervista.org	126,864	25.33%
dlinkddns.com	12,469	20.17%
sg-host.com	9,154	64.43%
sheridanc.on.ca	6,034	16.33%
uri.edu	1,095	60.04%
wixsite.com	1,063	35.12%
flcc.edu	629	51.25%

Table 1: CT logs are an effective data source for username enumeration. Seven websites leaked thousands of usernames through the subdomains on their certificates. We also show the percentage of the usernames for each website which include a popular U.S. surname or given name.

Llynda More Boots is an MLM company that provides its "independent representatives" with a subdomain, such as `deborahjones.llyndamoreboots.com`. We identified 376 members' subdomains containing both a given name and surname. On one hand, this may be intentional: some of the participants advertise themselves as independent representatives on their Facebook page or elsewhere in their online presence. On the other hand, it is not clear that affiliates understand that their names will be *permanently associated* with a multi-level marketing scheme, even if they decide to leave the program at any point in the future.

Realtors, Doctors, and other Businesses Not all websites that include users' names within subdomains are necessarily harmful. We find many examples of business websites that list the names of real estate agents, doctors, and other professionals. These websites advertise individual users' businesses, whose names are likely part of their brand. `lizroberts.silvercreekrealty.com` and `rickmccracken.findmytrianglehome.com` are examples of such sites.

2.2 Usernames

We observe that websites often use usernames as subdomains. Some websites obtain individual certificates for every user that registers on their site instead of obtaining a wildcard certificate (Section 4.1). Anyone can enumerate the usernames of users on these websites by querying the domains in CT logs.

Based on our observations, we hypothesize that users will often include their given name or surname when allowed free selection of a username. We verify this by analyzing the Xato 10 Million username/password dataset [5], and find that 20.89% of these usernames include a surname or given name.

Methodology Since many usernames contain users' real names, our query to the Censys dataset is the same as in Section 2.1. After identifying which websites embed usernames in subdomains, we return to Censys and collect all usernames, including those which do not contain a user's real name.

Table 1 shows seven domains that leak usernames on certificates. Collectively, our query technique found over 130,000 usernames across seven websites. This table is non-exhaustive; many websites appeared to include usernames, but could not be verified as they were no longer hosted online. We use these cases to stress the

[1] This also conveniently filters out domains that use common nouns that also happen to be surnames, such as `green.americanexpress.com`.

permanence of leaked data in CT logs; such data can be queried *even after the original data source ceases to exist.*

2.3 Email Addresses

After discovering users' names and usernames, we now search for user contact information in CT logs, via email addresses.

Methodology The first part of an email address is often self-selected or assigned by an organization. We use the same methodology described in Section 2.2. We then search for subudomains that also include popular email providers, such as "gmail.com" and "yahoo.com".

Compose DB We identified one example of email address leakage. IBM Compose [15] is a cloud-based platform for hosting a suite of databases. It enumerates users' email addresses as immediate subdomains under `composedb.com`, replacing "@" and "." with hyphens. Extracting the first subdomain and searching for "-com", we identified 5,861 distinct email addresses. Many email addresses came from free email services; 1,622 addresses were from "`gmail.com`", 118 from "`hotmail.com`", 78 from "`yahoo.com`", and 59 from "`outlook.com`".

With private email addresses, users may be unaware that their email activity is monitored and permanently logged. Almost half of the Compose DB email addresses (2,646) were from "`ibm.com`" itself. This is a particularly worrisome example, as it reveals email addresses and possible usernames of employees of IBM. Individuals may not care if someone learns their work-associated email address, but companies are potentially put at risk if someone can enumerate their employees [23], and access to employees' usernames creates opportunities for social engineering and spearphishing [14].

3 ENTERPRISE INFORMATION LEAKAGE

3.1 Business Relationships

Relationships between businesses are sometimes kept private. Services may not want competitors poaching their clients, and clients may wish to maintain a competitive edge over their competitors. We show that poor subdomain choice can leak information about what clients a service hosts.

Methodology We consider the top 100,000 most popular domains, according to the Alexa rankings [3], as viable clients or services. We look for the presence of those "target" domains within subdomains of other domains, such as the toy example `google.com.apple.com`. We then investigate the resulting set of domains for outliers by looking at which domains have the highest number of unique subdomains, and which domains have the most unique targets within their subdomains. Dominating both categories was the domain "`cas.ms`".

Microsoft CAS Microsoft Cloud App Security (CAS) [21] is a cloud security monitor that features a reverse proxy; when utilized, domains of external services such as "sharepoint.com" are replaced with domains similar to "sharepoint.com.us.cas.ms" [22]. 77,825 of these domains appear on certificates issued by Microsoft and are present in CT logs. Of these, many include the customer purchasing CAS as an additional prefix before the service being accessed; "`bryantstrattoncollege-my.sharepoint.com.us2.cas.ms`" reveals that Bryant & Stratton College is (or was) a CAS customer. We found over 4000 CAS customers, including Canary Telehealth, Canterbury College (Waterford), Embassy Management LLC, GameStop, and Star Financial Bank.

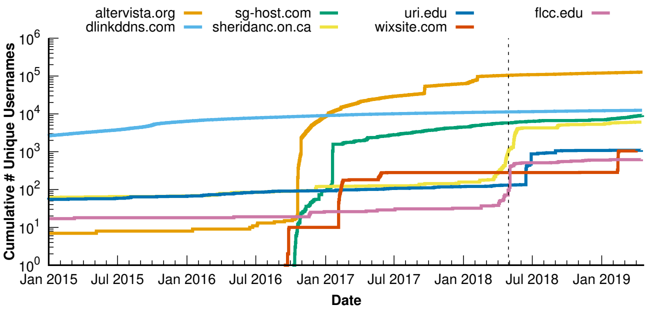

Figure 1: We can see changes to user growth over time by plotting the number of unique usernames seen on a domain up to each day. Here, we plot user growth for the domains in Table 1. Google Chrome requires all certificates issued after April 30, 2018 (noted by the vertical black line) to be included in CT logs.

3.2 Internal Domains & Unannounced Products

Methodology We again look for the top 100,000 most popular Alexa domains as subdomains. Using WHOIS data, we use the technique described by Cangialosi et al. [6] to find instances where the real domain and the domain embedded within a subdomain are owned by the same entity.

Discovery Inc. After applying our methodology, we see that the domain with the highest number of unique subdomains (25,346) is "`dsc.tv`". This domain is owned by Discovery Inc., parent company to multiple television channels. Among the subdomains are internal QA and staging servers, prefixed with Discovery Inc. properties ("`foodnetwork.com.staging-images.i.dsc.tv`"). Many of these domains begin with one of 27 additional subdomain prefixes, including "admin", "api", "metrics", and "service".

Seven of these prefixes contain the tokens "xbox", "playstation", or "samsungtv", revealing the development of Discovery applications for Xbox, PlayStation, and Samsung devices. Discovery released their Discovery GO application for Samsung smart TVs on June 27, 2018 [8]. The first `dsc.tv` certificate with a subdomain including "samsungtv" was issued on October 25, 2017, a full 8 months prior to the application's release on Samsung devices. In this case, CT logs exposed the development of a project prior to its public disclosure.

3.3 Measuring User Growth

Information on user growth can be valuable to a website's competitors looking to gain a larger share of the market. Recall Table 1, which lists websites that allow for username enumeration through CT logs. Every time a user registers a new username, a certificate must be issued to authenticate their new subdomain. We can use the issuance dates of these certificates to determine when new users signed up for each platform.

Methodology Use the same methodology from Section 2.2 to gather the certificates for every domain in Table 1. For every username, find the first certificate (by timestamp) issued that includes that subdomain. Once we find the genesis date for every username, we can plot how many unique usernames have been seen by a given day. From there, we can infer how the rate of new user adoption changes over time. The growth charts of the domains in Table 1 can be seen in Figure 1. Note the sharp inclines on this log-scale plot, indicating brief periods of exponential user growth.

4 DISCUSSION

4.1 Potential Solutions

Leaked information presented in this paper will be stored in CT logs indefinitely. However, there are many ways to prevent private information from leaking into CT logs in the first place.

Wildcard Certificates A certificate issued to "`*.example.com`" can be used to authenticate any subdomain in place of the wildcard. A wildcard can only be used to conceal one subdomain level, and that level must be the leftmost subdomain of the domain. While the domain "`username.example.com`" is valid for the above example, "`www.username.example.com`" is not. Domain administrators may need to alter their subdomain naming scheme if they wish to take advantage of wildcard certificates.

Private Subdomains Eskandarian et al. provide an augmentation to Certificate Transparency, allowing for the use of private subdomains [10]. The CT log stores a domain's owner, and a *cryptographic commitment* to a subdomain, without revealing the subdomain itself. The associated decommitment is provided as proof that the subdomain was appropriately logged in the CT log. Most examples of leaked information in this paper could be concealed under this scheme, though we note that websites may still be vulnerable to timing leaks as discussed in Section 3.

Education It remains unclear whether administrators are aware that CT logs store information permanently. User study research could provide insight into how administrators make decisions about subdomain structure. Such research would also help inform best practices for educational outreach to administrators who have been found leaking information through CT logs. Additionally, users can be taught to exercise caution when registering on a new website. If the user does not want to risk permanent association with the site, they should register under a unique username that includes no personal information.

4.2 Other Queries

Phone Numbers To investigate whether users' phone numbers were leaked on domains in CT logs, we queried for domains that contained 10-digit numbers separated by hyphens (*ddd-ddd-dddd*). No leakage was found, but we did find many businesses who use their phone number as their domain, such as `250-565-5024.com` (an alias for `rogerkollner.com`, a realtor's site). We do not consider these numbers leaked, as they were intentionally chosen to represent their company's online presence.

We did find two examples of domains that Google Safe Browsing [13] reports as malicious: `online-computer-support-1-844-711-9555.xyz` and `800-346-3454.tk`. We also found 74 unique phone number domains with the TLDs .ga, .ml, .cf, .tk, and .gq, five TLDs identified by Spamhaus for their association with sending internet spam [1]. While not flagged by Safe Browsing, the domains `call-on-1-866-389-1479-for-pc-support.tk`, `safari-currupt-1-888-243-1517.ga`, and `virus-alert-from-pc-call-1-844-204-9149.ml` have language consistent with computer support scams. Future work investigating the link between phone scams, internet scams, and domains with phone numbers could provide new insights into the spam ecosystem.

Non-Domains The Subject and Subject Alternate Name fields on certificates usually contain valid domains, but sometimes include other information. We investigated the content of these non-domain values for potential leaks. 18,905,772 fields were IPv4 addresses. After removing these, we were left with 4,149,763 unique values. Many of these had pseudo-TLDs, including "`.local`" (1,469,111), "`.default`" (370,429), "`.internal`" (370,090), and "`.localdomain`" (28,944). These domains clearly are not intended to be exposed to the wider web, as they have non-functioning TLDs outside of their local deployments.

Publicly revealing internal subdomains risks exposing projects, internal infrastructure, and in some cases the scale of resources being dedicated to them. As a concrete example, we see 783 distinct subdomains of `google.com.internal`, the immediate subdomains of which appear to be project names. We observe 34 distinct projects, including Google Cloud Engine (collectively spanning 674 distinct domain names), and a project referred to as "hoverboard" (sadly spanning only 2 domain names).

5 CONCLUSION

Certificate Transparency logs offer unprecedented insight into the certificate ecosystem. On the one hand, this allows the browser and security community to hold certificate authorities responsible, and permits novel techniques that require a global view of certificates [17]. On the other hand, too much or misunderstood transparency can have unintended consequences.

In this paper, we have identified some of the potentially negative consequences of CT's transparency, requiring us to look no further than the domain names in CT logs. As proofs of concept, we gathered leaked user and enterprise information, including names, usernames, email addresses, business relationships, and unreleased products. To further demonstrate the power of CT logs as a longitudinal dataset of leaked information, we inferred user growth rates from the dates that certificates were issued with user-leaking domain names.

There is likely much more unintended leakage of information present in CT logs today; this paper serves as the first step towards better understanding—and ultimately protection against—unintentional information leakage through public certificate logs. Without intervention, the amount of private information permanently on display to the public will only increase. Further research characterizing the information present in CT logs and developing solutions for logging private subdomains, will all be vital to stem the flow of private information they leak.

ACKNOWLEDGMENTS

We thank Taejoong Chung, David Choffnes, Alan Mislove, Christo Wilson, and the anonymous reviewers for their helpful feedback. This work was supported in part by NSF awards CNS-1564143 and CNS-1901325.

REFERENCES

[1] 2018. The Spamhaus Project: The World's Most Abused TLDs. https://www.spamhaus.org/statistics/tlds/.

[2] Pieter Agten, Wouter Joosen, Frank Piessens, and Nick Nikiforakis. 2015. Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. In *Network and Distributed System Security Symposium (NDSS)*.

[3] Alexa Top Sites API [n.d.]. Alexa Top Sites API. https://aws.amazon.com/alexa-top-sites/.

[4] Bharath. 2017. Certificate Transparency Part 3 – The dark side. Online: https://blog.appsecco.com/certificate-transparency-part-3-the-dark-side-9d401809b025.

[5] Mark Burnett. 2015. Today I Am Releasing Ten Million Passwords. https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495.

[6] Frank Cangialosi, Taejoong Chung, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2016. Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem. In *ACM Conference on Computer and Communications Security (CCS)*.

[7] Gurpreet Dhillon, Lemuria Carter, and Javad Abed. 2016. Defining Objectives for Securing the Internet of Things: A Value-Focused Thinking Approach.

[8] Discovery's TV Everywhere "GO" Apps Now Available On Select Samsung Smart TVs 2018. Discovery's TV Everywhere "GO" Apps Now Available On Select Samsung Smart TVs. https://corporate.discovery.com/discovery-newsroom/discoverys-tv-everywhere-go-apps-now-available-on-select-samsung-smart-tvs/.

[9] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. 2015. A Search Engine Backed by Internet-Wide Scanning. In *ACM Conference on Computer and Communications Security (CCS)*.

[10] Saba Eskandarian, Eran Messeri, Joseph Bonneau, and Dan Boneh. 2017. Certificate transparency with privacy. *Proceedings on Privacy Enhancing Technologies* 2017, 4 (2017), 329–344.

[11] Federal Trade Commission. [n.d.]. Multilevel Marketing. Online: https://www.ftc.gov/tips-advice/business-center/guidance/multilevel-marketing.

[12] Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle. 2018. In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements. In *Passive and Active Network Measurement Workshop (PAM)*.

[13] Google Safe Browsing [n.d.]. Google Safe Browsing. https://safebrowsing.google.com.

[14] Grant Ho, Aashish Sharma, Mobin Javed, Vern Paxson, and David Wagner. 2017. Detecting Credential Spearphishing Attacks in Enterprise Settings. In *USENIX Security Symposium*.

[15] IBM. [n.d.]. IBM Compose. Online: https://www.ibm.com/cloud/compose.

[16] Panagiotis Kintis, Najmeh Miramirkhani, Charles Lever, Yizheng Chen, Roza Romero-Gómez, Nikolaos Pitropakis, Nick Nikiforakis, and Manos Antonakakis. 2017. Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse. In *ACM Conference on Computer and Communications Security (CCS)*.

[17] James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers. In *IEEE Symposium on Security and Privacy*.

[18] Ben Laurie, Adam Langley, and Emilia Kasper. 2013. Certificate Transparency. RFC 6962. https://www.ietf.org/rfc/rfc6962.txt

[19] Mark Kantrowitz. [n.d.]. List of Common Female Names. Online: https://www.cs.cmu.edu/afs/cs/project/ai-repository/ai/areas/nlp/corpora/names/female.txt.

[20] Mark Kantrowitz. [n.d.]. List of Common Male Names. Online: http://www.cs.cmu.edu/afs/cs/project/ai-repository/ai/areas/nlp/corpora/names/male.txt.

[21] Microsoft. [n.d.]. Microsoft Cloud App Security overview. Online: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security.

[22] Microsoft. [n.d.]. Protect apps with Microsoft Cloud App Security Conditional Access App Control. Online: https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad.

[23] Kevin Mitnick and William L. Simon. 2002. *The Art of Deception*. Wiley Publishing Inc.

[24] Mozilla CT Policy 2014. PKI:CT. Mozilla Wiki. https://wiki.mozilla.org/PKI:CThttps://wiki.mozilla.org/PKI:CT.

[25] Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch. 2018. The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem. In *ACM Internet Measurement Conference (IMC)*.

[26] Ryan Sleevi. 2016. Announcement: Requiring Certificate Transparency in 2017. Certificate Transparency Policy. https://groups.google.com/a/chromium.org/forum/topic/ct-policy/78N3SMcqUGw.

[27] United States Census Bureau. [n.d.]. Decennial Census Surname Files. Online: https://www.census.gov/data/developers/data-sets/surnames.html.

[28] Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman. 2016. Towards a Complete View of the Certificate Ecosystem. In *ACM Internet Measurement Conference (IMC)*.

A DOMAIN EXAMPLES

Domain	Information Type	Paper Section
jessicaroman.llyndamoreboots.com	Name	2.1
brooksessions.llyndamoreboots.com	Name	2.1
richardgray.silvercreekrealty.com	Name	2.1
tammygraffam.benchmarkrealtytn.com	Name	2.1
dawnhooper.findmytrianglehome.com	Name	2.1
trudy1961.altervista.org	Username	2.2
dan1337.altervista.org	Username	2.2
nilrikson.dlinkddns.com	Username	2.2
felix-krueger.dlinkddns.com	Username	2.2
www.justinf2.sg-host.com	Username	2.2
northeastpork.nater2.sg-host.com	Username	2.2
mail.ixd0959.firebird.sheridanc.on.ca	Username	2.2
cpanel.vermgaur.dev.fast.sheridanc.on.ca	Username	2.2
laurafgagnon.vps.cs.uri.edu	Username	2.2
www.jlefoley.vps.cs.uri.edu	Username	2.2
www.pinedarodrigo68.wixsite.com	Username	2.2
cashforautojunk.wixsite.com	Username	2.2
jgoodwin9.csc.flcc.edu	Username	2.2
webdisk.wmclaughlin.csc.flcc.edu	Username	2.2
...5ec4ad3dcc3d.tfranklin-us-ibm-com.composedb.com	Email	2.3
...f27d2632ee15.ahmedgalalmohamed2016-gmail-com.composedb.com	Email	2.3
...affd-4e43a008cd48.james-silvester-uk-ibm-com.composedb.com	Email	2.3
...4e0c-854d-a000382ad4ac.jainrajeev1906-yahoo-com.composedb.com	Email	2.3
*.hunterindustries365.sharepoint.com.us2.cas.ms	Business Relationship	3.1
*.charlesriverlabs.sharepoint.com.us2.cas.ms	Business Relationship	3.1
*.westernalliancebank-my.sharepoint.com.eu.cas.ms	Busiiess Relationship	3.1
*.bryantstrattoncollege-my.sharepoint.com.us.cas.ms	Business Relationship	3.1
*.snapfinancellc.sharepoint.com.eu.cas.ms	Business Relationship	3.1
xbox.travelchannel.com.qa-anupam1.i.dsc.tv	Internal Information	3.2
services.media.dp.discovery.com.qa-1442.i.dsc.tv	Internal Information	3.2
samsungtv.foodnetwork.com.qa-authtesting.i.dsc.tv	Internal Information	3.2
playstation.animalplanet.com.qa-globallogic.i.dsc.tv	Internal Information	3.2
admin.hgtv.com.qa-core.i.dsc.tv	Internal Information	3.2
www.817-237-0000.com	Phone Number	4.2
*.800-420-0420.biz	Phone Number	4.2
031-990-6600.co.kr	Phone Number	4.2
www.virus-alert-from-pc-call-1-888-243-1517.gq	Phone Number	4.2
4-best-deal-call-562-375-4981.com	Phone Number	4.2
877-623-7190.plumber-services.consumer-assistant.com	Phone Number	4.2
call-microsoft-root-harddrive-error-toll-free-1-888-442-8735.us	Phone Number	4.2
cpanel.safari-currupt-1-888-243-1517.ga	Phone Number	4.2
...-1553827241-18.c.hoverboard-staging-test.google.com.internal	Non-Domain	4.2
video-omh2.c.lb-project-cuj.google.com.internal	Non-Domain	4.2
lb-receiver-asia-southeast1-a-3.c.gce-blackbox.google.com.internal	Non-Domain	4.2
instance-1.c.extended-arcana-171411.internal.google.internal.	Non-Domain	4.2
google-cloud-postgresql.us-east1-b.c.argon-fx-237719.internal	Non-Domain	4.2
kubernetes.default.svc.cluster.local	Non-Domain	4.2
ucp-controller.kube-system.svc.cluster.local	Non-Domain	4.2
C867-La-Ferriere-08258.aaa.local	Non-Domain	4.2
router-internet.default.svc.cluster.local	Non-Domain	4.2
www.default-domain4.tld	Non-Domain	4.2