# THE DOMAINTOOLS REPORT

## 2015 SPECIAL EDITION
## BULK DOMAIN REGISTRATION AGENTS

## SUMMARY

In the first DomainTools Report, published in the spring of 2015, we examined concentrations of malicious activity along several specific dimensions in order to identify "hotspots" across the Internet. The dimensions identified in that study were Top Level Domain, country of IP hosting, Registrar Whois Privacy Service, and domain registrant free email provider. We found isolated concentrations of malicious activity (botnet, spam, phishing, malware) in each of those categories, which could provide security practitioners with useful leads in identifying cybercrime networks or activities.

For this supplement, we again sought concentrations of malicious activity, but here we examined the role of what we term "Bulk Domain Registration Agents" in the creation of dangerous domains. Sometimes referred to as "bulk domain resellers," these entities exhibit a specific pattern of behavior:

>> They register large numbers of domains (our threshold was 1,000 domains)

.>> They register the domains with one set of identifying data, then after a very short time (often just a few minutes) change the registration details, en masse, to different values

>> They repeat this cycle

We found many examples. However, it is worth examining how this phenomenon came to our attention in the first place.

When the Anthem Healthcare breach broke in early 2015, it was one of the largest breaches to date, with some 80 million records stolen. A breach of this magnitude invites a great deal of scrutiny, and indeed there was excellent forensic analysis provided by cybersecurity firms such as Crowdstrike, and researchers such as journalist Brian Krebs; their research shed light on the attackers' methodology and resources.

A key domain in the attack, we11point[.]com (note the intentional misspelling), spoofed legitimate infrastructure in order to capture employee credentials (Wellpoint was Anthem's previous name). This domain was found to have been registered by a bulk registration agent, identified by its email address on the domain's initial Whois record. We decided to investigate this and other such agents to determine whether there was an identifiable pattern linked to large-scale malicious activity, or if this was an isolated instance. The results were illuminating.

## METHODOLOGY

Using the criteria described above, we created queries that mined the DomainTools database to identify likely BDRAs (Bulk Domain Registration Agents), yielding 233 initial candidates. We then individually examined these registrants to cull out false positives such as legitimate domain portfolio transfers. Of the remaining set of 122 BDRAs, we examined all domains that were initially registered to these agents.

We then compared the BDRA-registered domains against the same blacklist sources we used for the original DomainTools Report.

These agents work at high volume. Among the interesting statistics we compiled:

>> The pool of 122 BDRAs were tied to a total of over 2.8 million domains
>> One BDRA had registered, as of August 2015, over 814,000 domains

It is worth acknowledging that a BDRA could use more than one email address, so it is possible that what we identified as separate BDRAs in some cases could be the same entity—but as the data show, the linking of the domains through the email address of record is useful whether or not there is a 1:1 mapping to an individual or entity.

### WHAT IT IS, WHAT IT ISN'T

We considered possible explanations for these patterns of behavior, and ruled out several possibilities (among our 122 identified BDRAs):

>> We don't believe this is an OpSec (Operational Security) practice. It is so easy to falsify identity on Whois records, or to use privacy, that the rapid registration change pattern doesn't make much sense as a means of covering one's tracks.

>> We don't believe it is legitimate domain speculation. Many of these domain names are typos or proper spellings of recognized brands. This tells us that these domains were not opportunistic registrations of valuable keywords.

## CONCENTRATIONS OF MALICIOUS ACTIVITY

Our hypothesis was that some BDRAs might show strong patterns of recurring malicious activity. Indeed, we found several examples of this—some with high absolute numbers of malicious domains, some with high concentrations (percentage) of malicious domains, and some with both. Looking across the pool as a whole:

>> We observed malicious density as high as 72% (i.e. approximately 7 out of every 10 domains registered by the BDRA were later blacklisted)
>> However, some had very low density of malicious activity (suggesting that some BDRAs really aren't closely connected to serious harm)
>> 56 of the 122 have malicious density exceeding 10%
>> Aggregate malicious density across all BDRAs is 13.6%.

To put this in perspective, average malicious density across all currently extant domains is around 2-5%, depending on which blacklist sources are referenced.

## BULK DOMAIN REGISTRATION AGENT PROFILES

For infosec teams, it can be extremely useful to profile an adversary in order to better defend against it. Profiles can help a security team understand the scale of the adversary's operations, common themes (if any) in their holdings, naming conventions, and more. By examining these, defenders can sometimes correlate attacks which seemed to be unrelated at first—that is, if Domain A attacked them, and "John Doe" owns A, if they can discern that the same adversary owns domains B through Z, they now have a lot more to go on. They can use firewalls or other systems to block domains A through Z and related infrastructure (IP addresses and name servers, for example) tied to the adversary.

Adversary profiles are also often a viable substitute for a positive attribution. Knowing the actual name, phone number, or physical address of a cybercriminal is not only not necessary, but often not even helpful, in defending against them. A threat actor's online track record and presence provide much more guidance on how to defend against them. This is worth bearing in mind any time the debate arises over whether attack attribution is worth pursuing.

The brief profiles listed on the right provide insight into the activities of some of the more interesting BDRAs we studied.

| | e59e[@]qq.com |
|---|---|
| 1 | Implicated in Anthem Hack |
| 2 | Involved in in registration of we11point[.]com |
| 3 | Involved in almost 130,000 domains |
| 4 | Malicious density over 38% (38 out of 100 domains were later blacklisted) |
| 5 | Currently listed in WHOIS for 45,089 domains |

| | li2384826402[@]yahoo.com |
|---|---|
| 1 | Implicated in Anthem Hack |
| 2 | Involved in registration of topsec2014[.]com and sharepoint-vaeit[.]com |
| 3 | Involved in over 58,000 domains |
| 4 | Malicious density of 21.6% (21 out of 100 domains were later blacklisted) |
| 5 | Currently listed on WHOIS for 15,746 domains |

| | rgreeyfue76gj[@]gmail.com |
|---|---|
| 1 | Implicated in Premera Hack |
| 2 | Involved in registration of prennera[.]com |
| 3 | Involved in registration of 6,200 domains |
| 4 | Malicious density of 21.5% (21 out of 100 domains were later blacklisted) |
| 5 | Currently listed in WHOIS in ZERO domains. A retired BDRA? |

### A CHINA SYNDROME?

A large number of high-volume and high-blacklist-percentage BDRAs appear to have a Chinese origin, based on their email addresses. Seven of the top 10 BDRAs by volume used the Chinese email services qq or 126, and of the BDRAs that had both high volume and high blacklist rates, around half have apparent Chinese username or email provider connections. Of course, the ostensibly Chinese identities could be spoofed, so if one were seeking an in-depth profile of a particular BDRA, further research would be prudent.

## TOP BDRAs, BY COUNT

This table shows those BDRAs with the highest overall domain counts. Note that the highest-volume BDRAs have very low blacklist rates. These BDRAs may be virtually free of connection to harmful activity (with such low blacklist rates, it's possible that those domains that were blacklisted were compromised legitimate domains). It is also possible that they are involved in nefarious activities outside the scope of these blacklists—sales of counterfeit goods would be one example. To be clear, we do not imply any such connection. Six of the top 10 by volume, however, have blacklist rates significantly higher than the Internet background levels.

| | REGISTRANT EMAIL | TOTAL DOMAINS | % BLACKLISTED |
|---|---|---|---|
| 1 | 31311604[@]qq.com | **813,962** | 0.11% |
| 2 | xujiqing[@]126.com | **209,659** | 0.01% |
| 3 | 20702176[@]qq.com | **149,915** | 6.06% |
| 4 | e59e[@]qq.com | **129,375** | 33.74% |
| 5 | 7519626[@]qq.com | **102,023** | 58.59% |
| 6 | 80010864[@]qq.com | **89,378** | 6.60% |
| 7 | adomainslimited[@]gmail.com | **65,078** | 2.38% |
| 8 | dt0598[@]outlook.com | **61,941** | 6.57% |
| 9 | dnsprotect[@]126.com | **61,334** | 0.15% |
| 10 | li2384826402[@]yahoo.com | **58,100** | 20.49% |

## TOP BDRAs, BY DENSITY OF MALICIOUS DOMAINS

These BDRAs have very strong patterns of connection to malicious activity. As our work on the DomainTools Reputation Engine has shown, when a given entity has a high rate of blacklisting, there is a strong likelihood that those domains connected to that entity that are not (yet) blacklisted are, nonetheless, likely to be harmful. Some of these high-blacklist-rate BDRAs operate at relatively low volume. Regardless, a security team could use a cross-indexed database of Whois records to develop a list of all domains registered by these BDRA email addresses, and then block all of those domains at the network perimeter or in email or web filters.

| | REGISTRANT EMAIL | % BLACKLISTED | # BLACKLISTED |
|---|---|---|---|
| 1 | easystreetmkt[@]gmail.com | **98.16%** | 1,762 |
| 2 | privatedomainservices01[@]gmail.com | **83.83%** | 1,954 |
| 3 | awx0529[@]hotmail.com | **68.87%** | 1,701 |
| 4 | dt22888[@]126.com | **64.84%** | 1,582 |
| 5 | yuanjinhua123[@]gmail.com | **61.10%** | 14,481 |
| 6 | 7519626[@]qq.com | **58.59%** | 59,775 |
| 7 | dallascustomersoffice[@]gmail.com | **56.41%** | 2,957 |
| 8 | fgikhhfgjeds[@]163.com | **54.53%** | 1,173 |
| 9 | macdougall.jesse[@]gmail.com | **50.89%** | 629 |
| 10 | 2429365[@]qq.com | **50.82%** | 6,648 |

## TOP BDRAs BY COMBINATION OF VOLUME AND DENSITY

This list comprises BDRAs that had both a high absolute number of domains and a high blacklist rate. We've listed BDRAs with at least 9,000 blacklisted domains, which amount to at least 20% of their domain registration portfolio. In other words, these entities represent high overall impact per individual (as represented by a registration email address). These, too, would be reasonable candidates for registrant-based filtering, as described above.

| | REGISTRANT EMAIL | BLACKLISTED DOMAINS | % BLACKLISTED |
|---|---|---|---|
| 1 | 7519626[@]qq.com | **59,775** | 58.59% |
| 2 | e59e[@]qq.com | **43,646** | 33.74% |
| 3 | unalee1127[@]outlook.com | **18,709** | 37.86% |
| 4 | dddpppeee[@]yahoo.com | **17,762** | 32.65% |
| 5 | paulzz[@]yeah.net | **14,690** | 35.92% |
| 6 | yuanjinhua123[@]gmail.com | **14,481** | 61.10% |
| 7 | quinnxaa[@]hotmail.com | **12,378** | 28.54% |
| 8 | li2384826402[@]yahoo.com | **11,902** | 20.49% |
| 9 | eicccsk[@]yahoo.com | **9,965** | 22.67% |
| 10 | seminaroqla[@]yahoo.com | **9,233** | 33.79% |

## CONCLUSIONS

This study represents a large-scale example of a methodology used by security practitioners daily: **mining cross-referenced domain profile information to identify connections and patterns among domains and the entities that control them**. One could create a blacklist, for example, by monitoring the registrations of high-volume BDRAs and automatically blocking all of the domains they register. At smaller scale, many companies create such blacklists based on malicious domain registrants that they have observed targeting their organizations. It is clear that there are patterns present in registration records that can be used to identify, track, and block various kinds of malicious activity online.

## ABOUT DOMAINTOOLS

DomainTools is the leader in domain name, DNS and Internet OSINT-based cyber threat intelligence and cybercrime forensics products and data. With over 14 years of domain name, DNS and related 'cyber fingerprint' data across the Internet, DomainTools helps companies assess security threat risks, profile attackers, investigate online fraud and crimes, and map cyber activity in order to stop attacks.

Our goal is to stop security threats to your organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. We collect and retain Open Source Intelligence (OSINT) data from many sources and we index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

DomainTools uses over 10 billion related DNS data points to build a map of 'who's doing what' on the Internet. Government agencies, Fortune 500 companies and leading security firms use our data as a critical ingredient in their threat investigation and cybercrime forensics work.

For more information about DomainTools' data and products, please visit our website at **www.domaintools.com**.