Criminal Abuse of Domain Names

Bulk Registration and Contact Information Access

Prepared by

Dave Piscitello and Dr. Colin Strutt

Interisle Consulting Group, LLC

17 October 2019

Interisle
Consulting Group

Executive Summary

Domain names that can be rapidly acquired, used in an attack, and abandoned before they can be traced are a critical resource for cybercriminals. Some attacks, including spam and ransomware campaigns and criminal infrastructure operation (e.g., "botnets"), benefit particularly from the ability to rapidly and cheaply acquire very large numbers of domain names—a tactic known as *bulk registration*. When cybercriminals can register hundreds or thousands of domain names in a matter of minutes, an attack can be widely distributed to make detection, blocking, and dismantling more difficult and prolonged.

Cybercrime investigation is always a race against the clock—the longer it takes to identify an attacker and block the attack, the more damage can be inflicted on more victims. Before the adoption by ICANN of a Temporary Specification ("Temp Spec") for handling domain name registration data in compliance with the European General Data Protection Regulation (GDPR), investigators had ready access to the contact information provided by domain name registrants ("Whois data"). This information, even when incomplete or inaccurate, facilitated rapid attack response both directly (when it correctly identified the attacker) and indirectly (by enabling "connect the dots" methods such as search-and-pivot).

The immediate effect of the Temp Spec since the GDPR took full effect on 25 May 2018 has been to severely limit access to domain name registrant contact information, most of which is now redacted by registries and registrars when they respond to Whois data queries. Although cybercrime investigators with proper authorization can petition a registry or registrar for the redacted information, this takes place on a glacial time scale compared to the "every second counts" imperative to limit the loss or harm caused by an attack.

The use of bulk registration to distribute attacks across hundreds or thousands of domain names in matters of minutes, coupled with the crippling of registration data access by the Temp Spec, presents cybercrime investigators with the dual impediments of harder-to-pursue criminal activity and harder-to-obtain information about the criminals.

For this report, Interisle researchers studied both aspects of this impediment:

- We studied samples of security events during which many thousands of domains were blocklisted in relatively short time frames.
- We identified registrars that offer bulk registration services and have large concentrations of blocklisted domains.
- We characterized the behavior of domain name registrants who engage in bulk registrations that are detected and blocklisted as criminal activities.
- We studied the way in which domain name registrants' use of privacy protection services or the redaction of Whois point-of-contact information inhibits or delays cybercrime investigation.

Our study confirms the hypothesis that cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domains for their attacks. The study identifies four specific registrars at which abusive registration activity appears to be concentrated. Our findings corroborate those of the 2017 ICANN report *Statistical Analysis of DNS Abuse in gTLDs* (SADAG).

Our study also confirms that ICANN's Temp Spec policy of redacting Whois point of contact information to comply with the GDPR significantly encumbers and delays cybercrime investigation. Working without

essential information, both real time and historical, investigators cannot make the necessary correlations to quickly and thoroughly map a criminal domain infrastructure or to attribute criminal activity to a perpetrator in time to prevent substantial harm to the victims of an attack.

Based on these findings, we make the following policy recommendations:

1. Validate domain name registration data.
2. Define "bulk registrant" as a new element of registration data for Whois.
3. Define an Acceptable Use Policy (AUP) that applies specifically to parties that register large numbers of domains.
4. Require registrants to apply for bulk registration services.
5. Distinguish domain names registered by legal entities from those registered by natural persons, classify parties that use bulk registration services as legal entities, and require unredacted access to the registration data of legal entities.
6. Maintain and publish a current list of validated bulk registrants.
7. Disallow registration transactions that involve large numbers of random-looking algorithmic domain names.
8. Disallow, for a period of one year, the re-registration of any bulk-registered domain name that has been used in a criminal cyberattack.
9. Provide the ICANN DAAR project with access to unredacted Whois data without rate limiting.

Implementing these recommendations will require the concerted and collaborative effort of every participant in the domain name registration system: ICANN, registries and registrars, government regulators, individual and institutional registrants, and cybercrime investigators. It may also require further study to establish thresholds and assess the effectiveness and feasibility of different implementation strategies.

We believe that committing to this effort is clearly within the scope of ICANN's obligation to operate "for the benefit of the Internet community as a whole" (see Bylaws, "Commitments"), which demands that it recognize a broad remit that extends to how a domain name (or other Internet identifier) is misused to point to or lure a user or application to content that is harmful, or to host content that is harmful.

Harmful content itself is not ICANN's concern; the way in which Internet identifiers are used to weaponize harmful content most certainly is.

Table of Contents

Table of Figures

Introduction

Domain names that can be rapidly acquired, used in an attack, and abandoned before they can be traced are a critical resource for cybercriminals. Some cyberattacks, including spam and ransomware campaigns and criminal infrastructure operation (e.g., "botnets"), benefit particularly from the ability to rapidly and cheaply acquire very large numbers of domain names—a tactic known as *bulk registration*. When cybercriminals can register hundreds or thousands of domain names in a matter of minutes, an attack can be widely distributed to make detection, blocking, and dismantling more difficult and prolonged.

Cybercrime investigation is always a race against the clock—the longer it takes to identify an attacker and block the attack, the more damage can be inflicted on more victims. Before the adoption by ICANN of a Temporary Specification for gTLD registration data ("Temp Spec") for handling domain name registration data in compliance with the European General Data Protection Regulation (GDPR) , investigators had ready access to the contact information provided by domain name registrants ("Whois data"). This information, even when incomplete or inaccurate, facilitated rapid attack response both directly (when it correctly identified the attacker) and indirectly (by enabling "connect the dots" methods such as search-and-pivot).

The immediate effect of the Temp Spec since the GDPR took full effect on 25 May 2018 has been to severely limit access to domain name registrant contact information, most of which is now redacted by registries and registrars when they respond to Whois data queries. Although cybercrime investigators with proper authorization can petition a registry or registrar for the redacted information, this provision is not uniformly provided by registries or registrars, and the response to such petitions are processed on a glacial time scale compared to the "every second counts" imperative that cybercrime first responders require to limit the loss or harm caused by an attack.

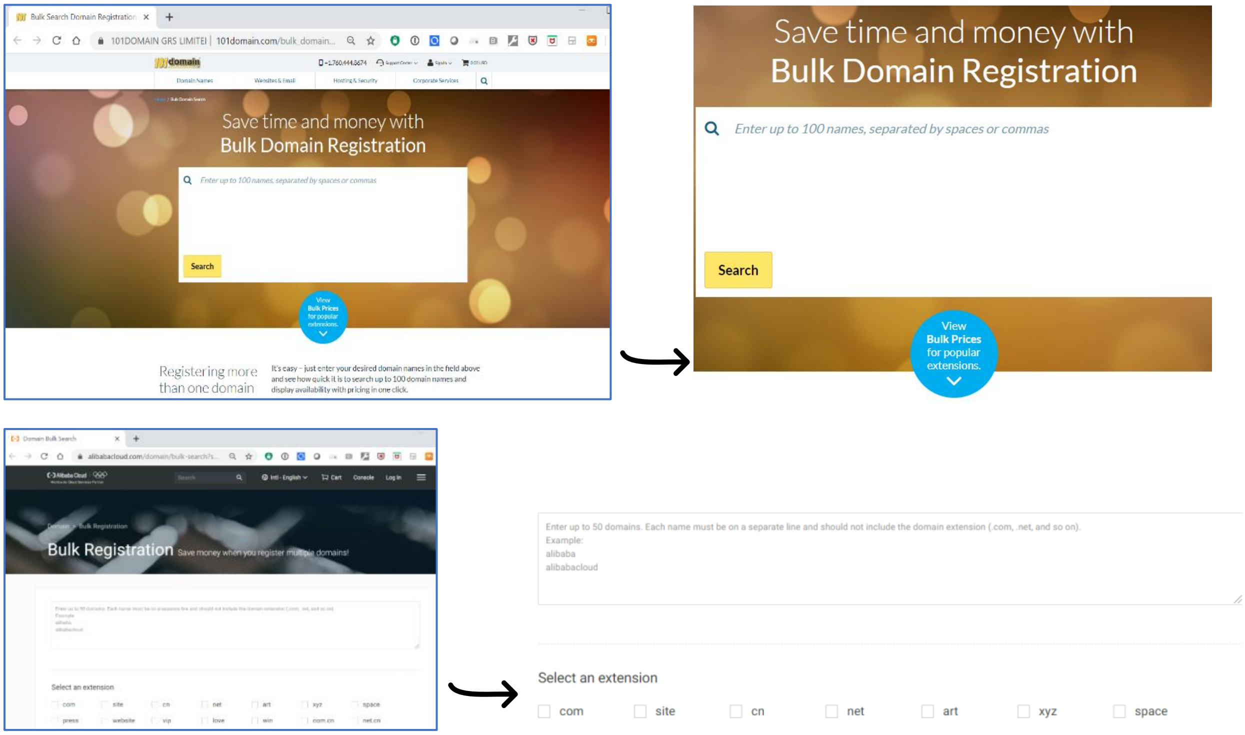
The use of bulk registration to distribute attacks across hundreds or thousands of domain names in matters of minutes, coupled with the crippling of registration data access by the Temp Spec, presents cybercrime investigators with the dual impediments of harder-to-pursue criminal activity and harder-to-obtain information about the criminals.

In this report, Interisle studied both aspects of this impediment. We hypothesized that cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domains for their attacks. We then studied samples of security events during which many thousands of domains were blocklisted in relatively short time frames, identified registrars where large numbers of blocklisted domains were concentrated, and characterized the behavior of domain name registrants who engage in bulk registrations that are detected and blocklisted as criminal activities. Using the same samples, we also studied the way in which domain registrants' use of privacy protection services or the redaction of Whois point-of-contact information inhibits or delays cybercrime investigation.

Our study confirms the hypothesis that cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domains for their attacks. Our study also confirms that ICANN's Temp Spec policy of redacting Whois point of contact information to comply with the GDPR significantly encumbers and delays cybercrime investigation. Based on these findings, we propose several policy recommendations.

A close look at bulk domain name registrations

The typical method of registering a domain name is to use a domain name registrar's web form. In cases where cybercriminals need to acquire very large numbers of domain names for the specific purpose of executing an attack, this is too slow and inefficient. Instead attackers look for domain name registrars or resellers that offer some means of automation through which requests for hundreds or even thousands of domain names can be submitted, e.g., a bulk web submission form, a file upload, a name suggestion tool that auto-generates large numbers of names, or an API.



Save time and money with Bulk Domain Registration

Enter up to 100 names, separated by spaces or commas

Search

View Bulk Prices for popular extensions.

Registering more than one domain

It's easy – just enter your desired domain names in the field above and see how quick it is to search up to 100 domain names and display availability with pricing in one click.

Bulk Registration Save money when you register multiple domains!

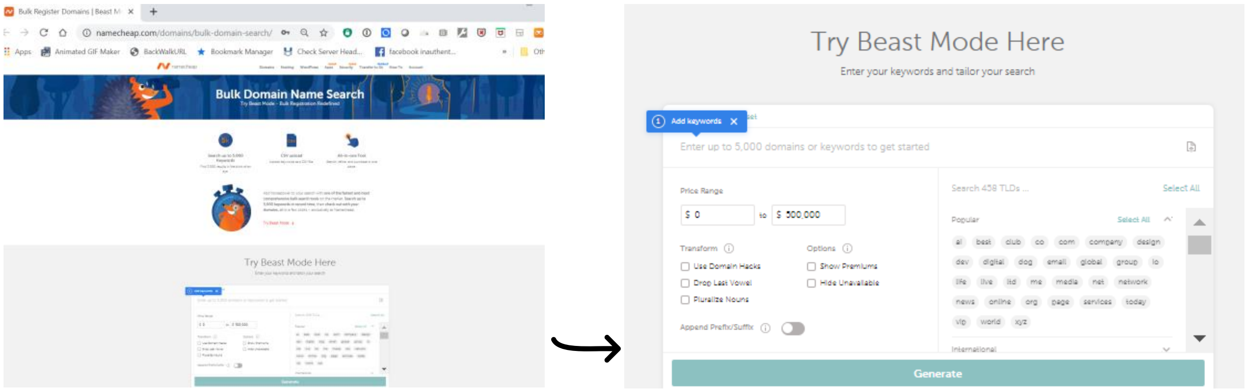
Enter up to 50 domains. Each name must be on a separate line and should not include the domain extension (.com, .net, and so on).
Example:
alibaba
alibabacloud

Select an extension

□ com □ site □ cn □ net □ art □ xyz □ space

Figure 1: Representative bulk domain registration web forms

For example, criminals who operate snowshoe spam campaigns will register and propagate spam from thousands of domains or IP addresses to thwart antispam measures. Figure 2 is representative of a web form that accommodates up to 5,000 names, provides name composition assistance, and allows the registrant to enter the amount of money he is willing to spend.



Bulk Domain Name Search

Try Beast Mode Here

Enter your keywords and tailor your search

Add keywords ×

Enter up to 5,000 domains or keywords to get started

Price Range $ 0 to $ 500,000

Transform: □ Use Domain Hacks □ Drop Last Vowel □ Pluralize Nouns

Options: □ Show Premiums □ Hide Unavailable

Append Prefix/Suffix

Search 459 TLDs ... Select All

Popular Select All

ai best club co com company design dev digital dog email global group io life live ltd me media net network news online org page services today vip world xyz

International

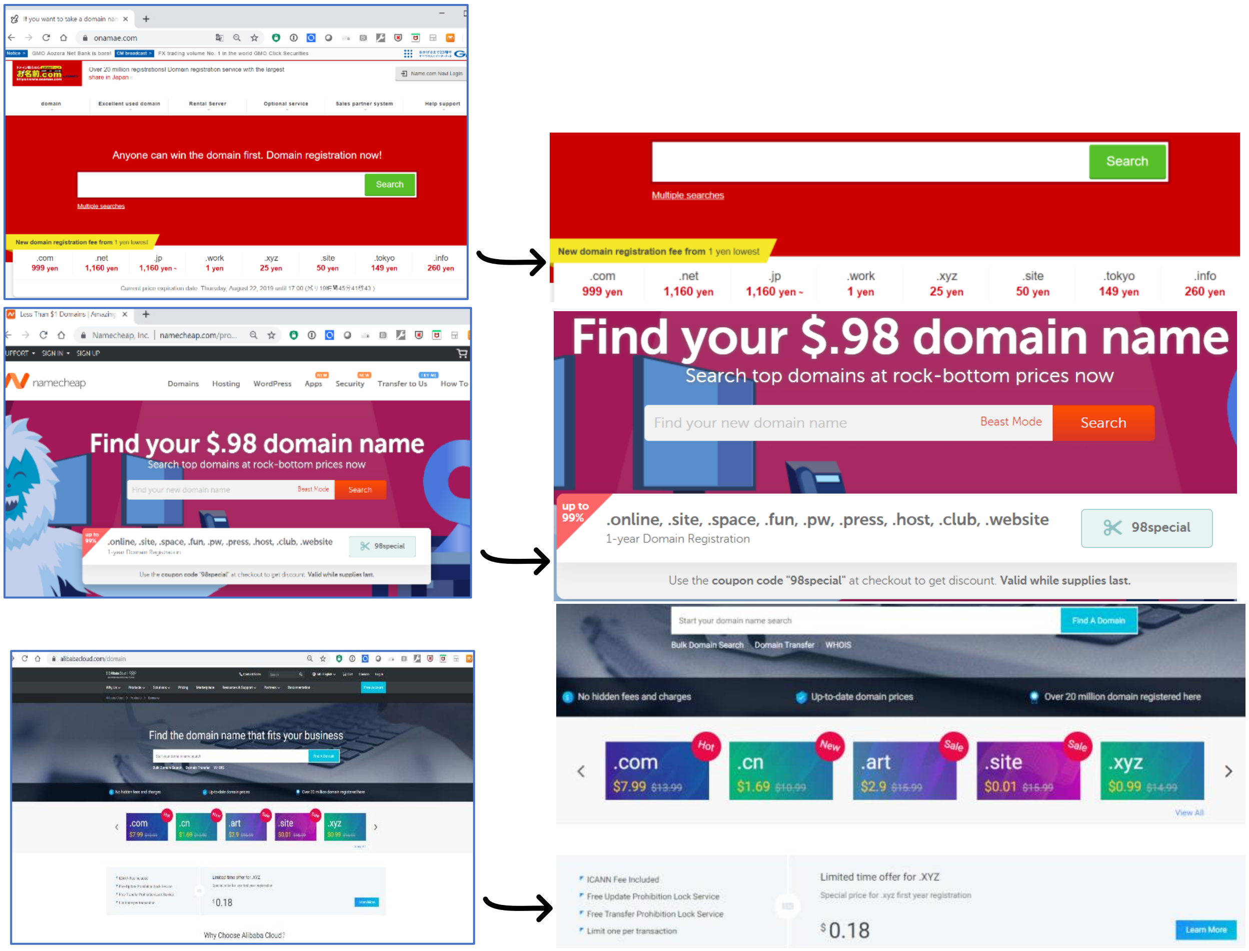
Generate

Figure 2: Web form for registration of up to 5000 domains in bulk

Domain names are dirt cheap

A simple search is all that is required to find registrars that offer gTLD registrations for less than $1 US (See Figure 3 for examples). Promotional pricing at certain registrars can be as low as 1 ¥ Japan ($.01 US, again, see Figure 3). Attackers can thus register thousands of domains routinely and cheaply. Bulk registration services provide the means whereby attackers can use thousands of domains for an attack knowing that when private sector investigators or law enforcement are able to have these domains suspended or seized, they can easily obtain thousands more. ICANN makes registrants responsible for the completeness and accuracy of their contact data, which is sometimes displayed in WHOIS services, and may be available to law enforcement under relevant process. Attackers can and do use fraudulently composed contact data and register domains repeatedly and thus make attribution a challenging task for law enforcement, private sector investigators and researchers.

First-year discounts are attractive to attackers. Unlike domain names that parties register for legitimate and typically long-term use, domains registered for attack or criminal purposes are disposable resources. They become less useful after first responders triage the attack by blocklisting a domain or URL or removing content. Triage is important as a containment strategy: it buys time to mitigate a vulnerability or threat.



onamae.com
Anyone can win the domain first. Domain registration now!
Search
Multiple searches
New domain registration fee from 1 yen lowest
.com 999 yen
.net 1,160 yen
.jp 1,160 yen ~
.work 1 yen
.xyz 25 yen
.site 50 yen
.tokyo 149 yen
.info 260 yen
namecheap
Domains
Hosting
WordPress
Apps
Security
Transfer to Us
How To
Find your $.98 domain name
Search top domains at rock-bottom prices now
Find your new domain name
Beast Mode
Search
up to 99%
.online, .site, .space, .fun, .pw, .press, .host, .club, .website
1-year Domain Registration
98special
Use the coupon code "98special" at checkout to get discount. Valid while supplies last.
alibabacloud.com/domain
Find the domain name that fits your business
Start your domain name search
Find A Domain
Bulk Domain Search
Domain Transfer
WHOIS
No hidden fees and charges
Up-to-date domain prices
Over 20 million domain registered here
.com $7.99 $13.99 Hot
.cn $1.69 $10.99 New
.art $2.9 $15.99 Sale
.site $0.01 $15.99 Sale
.xyz $0.99 $14.99
View All
ICANN Fee Included
Free Update Prohibition Lock Service
Free Transfer Prohibition Lock Service
Limit one per transaction
Limited time offer for .XYZ
Special price for .xyz first year registration
$0.18
Learn More
Why Choose Alibaba Cloud?

Figure 3: Examples of cheap domain name registrations

Purpose of this study

Private sector security professionals, cybercrime researchers, and law enforcement (hereafter, "Investigators") *can* use the attacker's attraction to bulk registrations to their advantage. Bulk registrations are often made under a single registrant. The registrations, whether 50, 100, or 5000, are created through one registrar. The contact data or other Whois data fields for the domains (name server, creation date…) is frequently the same for the all domains that a criminal registers via a single account. Complete Whois data, when it has not been redacted or cloaked using a privacy protection service, provides several data elements that investigators can use to search Whois records, either by querying for registrations using the Whois protocol or by searching Whois records that are collected for investigative purposes by the investigators themselves, or by commercial or private threat intelligence security systems.

Our first objective is to study samples of security events where many thousands of domains were blocklisted in a relatively short time frame. We *intend to study registrars that offer bulk registrations and also exhibit high concentrations of blocklisted domains for the Top-level Domains* in our study. We intend to study the behaviors of domain registrants of the bulk registrations as well. From our findings, we make recommendations for ICANN Consensus Policy consideration.

As a second objective, using the same samples, we intend to demonstrate how a domain registrant's use of *privacy protection services or redaction of Whois point-of-contact information to comply with the EU GDPR or ICANN's Temp Spec introduce an additional level of complexity for investigators*, who must request disclosure of the private record or "non-public Whois". From our findings, we again make recommendations for ICANN Consensus Policy consideration.

To achieve these objectives, we demonstrate how investigators use Whois records to associate portfolios or sets of domains with perpetrators of cyberattacks or cybercrimes. We show how investigators can search across Whois registration data sets and beyond, into other searchable data sets, to identify suspects even in circumstances where the data provided during a domain name registration is fraudulently composed. We demonstrate how other domain registration data, e.g., creation dates, are also relevant to investigations of this kind. We also demonstrate how investigators can use domain registration data as search arguments into Internet addressing databases, reputation systems, content archives, and social media.

For these objectives, we use sets of blocklist data from dates before and after the adoption of ICANN's Temp Spec.

A focus on cybercrime

In this report, we focus on misuse of domain names in connection with cybercrimes. The domain names in our samples were blocklisted for their association with phishing, malware, spam, or botnet activities. These are all identified as cybercrimes in the Council of Europe Convention on Cybercrime (Budapest Convention), an International Treaty with broad adoption.

Methodology

For the generic Top-level Domains (gTLDs) we studied, we obtained composite blocklist and reputation data from a variety of threat intelligence and reputation lists, noted below. We looked at domains that had been listed by one or more of the following sources:

- APWG eCrime eXchange anti-phishing database
- SURBL URI reputation data
- Seclytics attack prediction platform
- PhishTank anti-phishing clearinghouse
- Malware Patrol intelligent threat data
- Stopbadware malware clearinghouse
- The Spamhaus Block List (SBL)
- Abuse.ch malware reputation data

For the ccTLD selected for our study, we used data obtained from the Spamhaus Project.

We used historical data, e.g., the Internet Archive, to complement and to further investigate the domain names in our composite blocklist data. We also attempted to retrieve web page snapshots, additional reputation data, malware signatures, or routing and hosting information from sources including:

- Domain Tools IRIS Investigation Platform
- CuteStat web statistics and valuation service
- MalwareURL.com malicious URL reporting site
- Stop Forum Spam reporting service for forum spam and blog spam
- Wikipedia for personality search

We also used search engines—Google, Yahoo!, and Bing—to find information associated with data elements from domain name registrations, Internet addresses, or autonomous systems that exhibited suspicious bulk registration behaviors.

Each data set contains lists of domain names that were blocklisted by one or more of the reputation data services. The relevant data in each domain name record for our study includes:

- available domain name registration data (the Whois record, full or redacted),
- the TLD,
- the length and composition of the 2nd level label,
- the date when the domain was initially blocklisted,
- the blocklist(s) that tagged the domain name as a security threat,
- available classification of the security threat (e.g., phishing, malware, spam), and
- the date when a domain was removed from a blocklist.

We looked for evidence of bulk registration misuse in five generic Top-level domains (gTLDs) and one country code TLD (ccTLD). We obtained samples from timeframes prior to and post May 25, 2018. This provided us with the opportunity to study any impact on investigation methods post adoption of the EU GDPR and the corresponding adoption of the ICANN Temp Spec by registrars and registries.

For our first objective, we analyzed our samples to profile bulk registration misuse from several perspectives. We identified:

1) the registrars where blocklisted domains are concentrated in the sample TLDs, to identify flocking behavior, or to identify registrars that attract cyber attackers,
2) where available domain name registration allowed, the registrants who had registered large numbers of blocklisted domains in the sample TLDs,

3) where observable, creation date patterns of blocklisted domains that identify instances where a registrant made use of a volume or bulk registration service,
4) where observable, distinct 2nd level label composition of blocklisted domains, to identify instances where a registrant made use of bulk submission or name suggestion tools, and
5) where observable, IP addresses and Autonomous Systems of blocklisted domains, to determine whether or not registrants hosted Internet services (DNS, email, web) to operators with reputations for criminal hosting.

These profiles are described in the report.

There are certain limitations to studies that use historical data. For example, investigations launched at the onset of an attack—phishing, botnet operation, malware distribution, or spam—typically have "original" samples of email or other messaging service messages: blocklist operators and investigators typically do not share email messages to comply with data protection or privacy regulations. Also, domain names under "live" investigation resolve in the public DNS: they haven't been blocklisted or suspended yet. Investigators can typically access and analyze web page content, scripts, and URLs.

For our second objective, we included pre- and post-GDPR and Temp Spec adoption (May 25, 2018) samples to demonstrate how policy changes to Whois interfere with first response and how they impede criminal or abuse investigations. Specifically,

1. We show that, for investigations of domains registered prior to May 25, 2018, we were able to employ publicly available domain name registrant information (e.g., point of contact data) from Whois to quickly profile and identify registrants with extraordinary numbers of blocklisted domain registrations.
2. We then compared the methods and results of (1) against methods that are available post-May 25, 2018, when point of contact information became unavailable using Whois queries.

Registry Analyses

We studied multi-day samples of composite blocklist data from .TOKYO, .XYZ, .CLOUD, .TOP, and .US. For these TLDs, we share our findings of the registrars with the highest concentrations of blocklisted domain names. Where the available domain registration data permit, we studied registrants that exhibit high concentrations of blocklisted domains and then made observations of bulk registration behaviors that characterize domain name misuse. We also studied hosting behavior, e.g., whether or not the registrant concentrated his hosted services at operators with reputations for exhibiting high concentrations of misuse or criminal activity across their allocated address spaces.

Our findings are based on the domains that were reported and incorporated into the composite blocklists during our sample time frames. It is quite likely that other domain names were registered by the suspects (registrants) in our study. Some of these may have eluded detection. Our suspects may be stockpiling these for future use. The registration data of some of these may be obscured behind privacy protection or redacted Whois records.

Domain name misuse in .TOKYO

We studied blocklisting activity in .TOKYO from December 12, 2018 through December 25, 2018. We found that 8,715 .TOKYO domain names had been blocklisted in those fourteen days. Spamhaus calculates a badness index, which is ratio of domains being observed in spam messages weighted by the size of the TLD. At the writing of this report, the badness index value for TOKYO was 19.4%. This is low compared to neighboring city .NAGOYA (62.4%), but significantly higher than city TLDs in other geographic regions—e.g., .LONDON (.04%), .PARIS (0.4%), .MELBOURNE (0.0%), .MOSCOW (3.7%), and .RIO (0.0%)—that have much lower badness indexes.

Registrars with high blocklist concentrations in .TOKYO

One ICANN accredited registrar, GMO Internet, Inc., accounts for more than 99% (8,713 of the 8,715) of the blocklisted domain names in our .TOKYO blocklist sample.

Registrar	IANA ID	Blocked Domains	Percent
GMO Internet, Inc. d/b/a Onamae.com	49	8,713	100.0
NameCheap, Inc.	1068	2	0.0

Table 1: Registrars with high blocklist concentrations in .TOKYO

Daily blocklisting activity

Chart 1 illustrates the daily blocklisting activity in .TOKYO during our study period. We used the earliest detection date reported by the reputation data feeds that comprise our composite blocklist data. On three dates, we noted blocklistings in excess of 1000 domains.

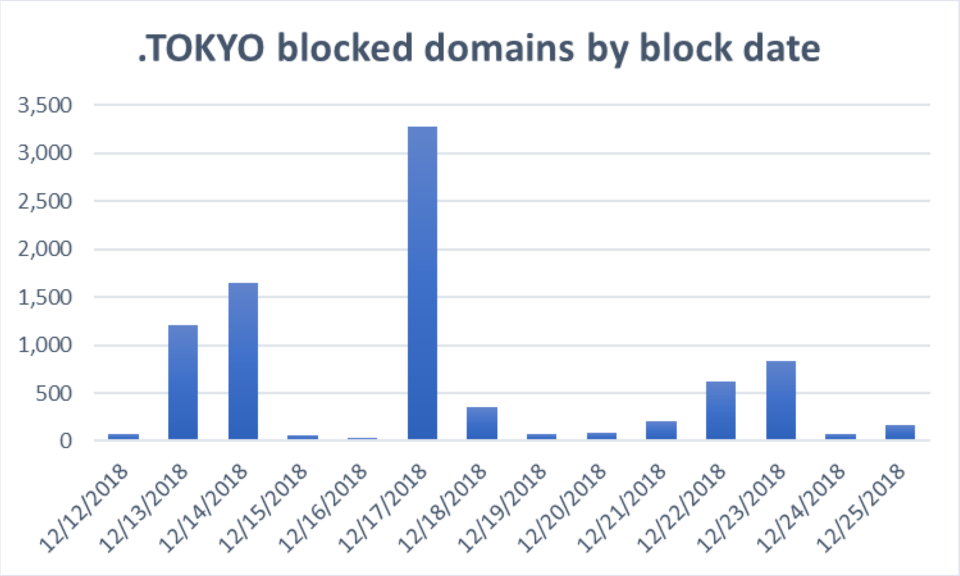


Chart 1: Earliest date of blocklisting of .TOKYO domains in sample

Insights from creation date

Chart 2 illustrates the creation (registration) date of the blocklisted names in our sample data. A large concentration of domain names that were blocked between 12/13/2018 and 12/25/2018 were also created in December 2018. Chart 2 also illustrates that criminal domains may not be blocklisted weeks or months following creation. This suggests that some criminals warehouse domains for later use.

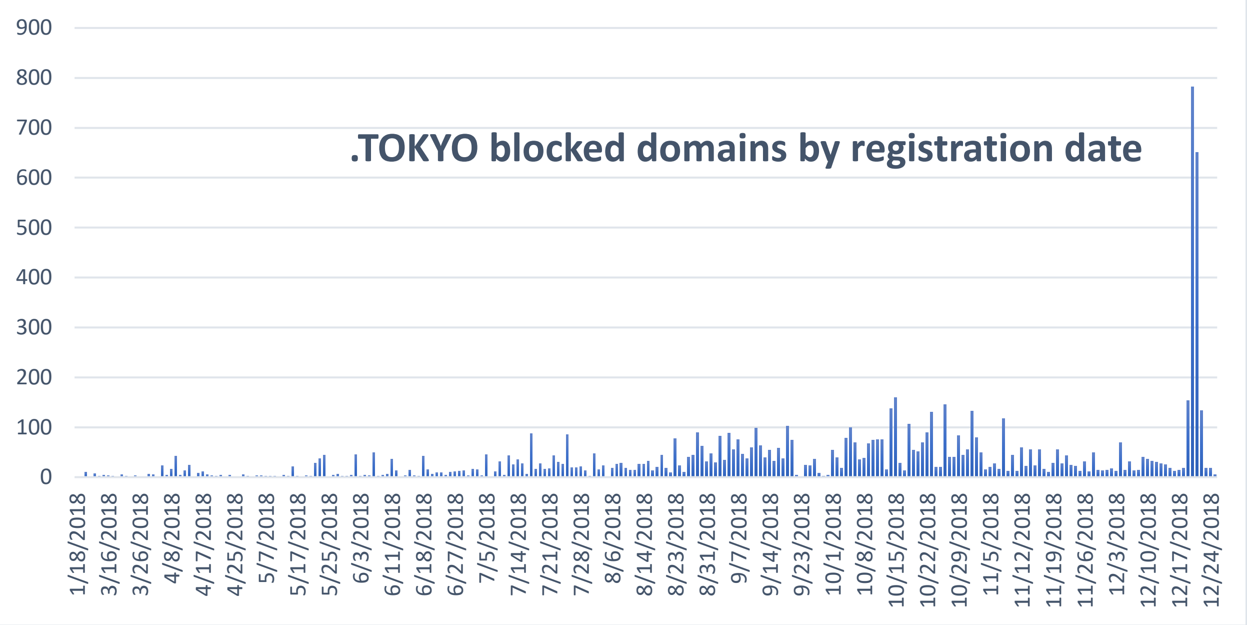


Chart 2: Blocklisted domains in .TOKYO, according to the domain creation date

Composition of 2nd level labels

Examining the length and composition of 2nd level labels may help investigators associate domains with a registrant, or to associate the registrant with some form of automated domain name registration behavior. In our study we looked for random-looking strings or strings that included recognizable English words, because such compositions suggest automation was used. In this sample, the majority of blocklisted domains were six or seven characters long. We found very few instances of labels containing recognizable English words (e.g., sexvideo.TOKYO). Nearly all of the 8,715 blocklisted domains in our sample exhibit patterns that are characteristic of random-looking domain names as explained in the article, Automating Detection of "Random-Looking" Algorithmic Domain Names:

- 6,927 2nd level labels had no hyphen. Of these, 2,397 had 7 alphanumeric characters, e.g., acjprtd.TOKYO, and 2,162 had 6 alphanumeric characters, e.g., fxkybx.TOKYO.
- A hyphen was present in 1,788 2nd level labels as the 5th character and 1,032 of these were of the form {4 alphanumerics, hyphen, 5 alphanumerics}, e.g., wt8h-vbzeu.TOKYO.

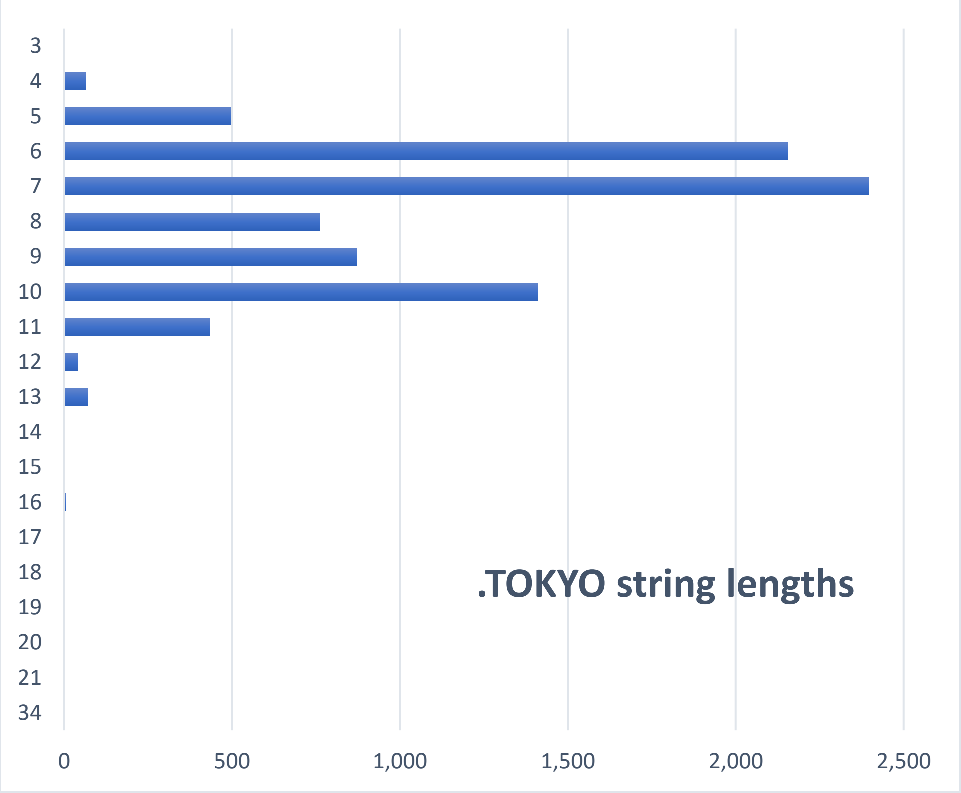


Chart 3: String lengths in .TOKYO blocklisted domains

The creation dates of the random-looking 6-character labels in Chart 4 suggest that these names are frequently registered in batches, beginning 12-Jul-2017 and ending 21 Dec-2018.

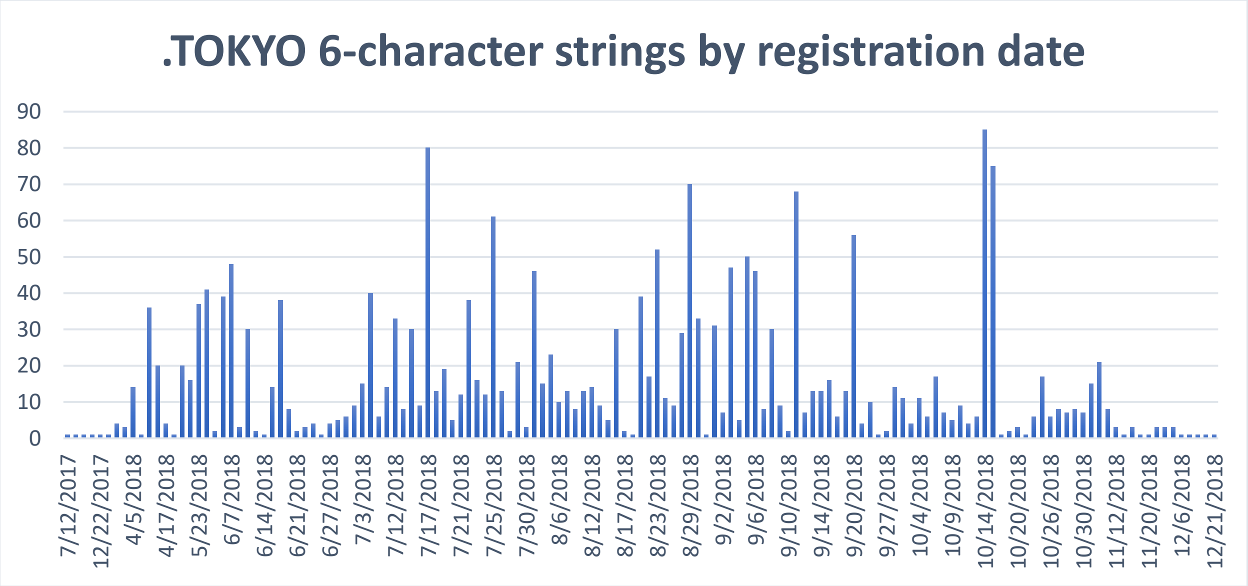
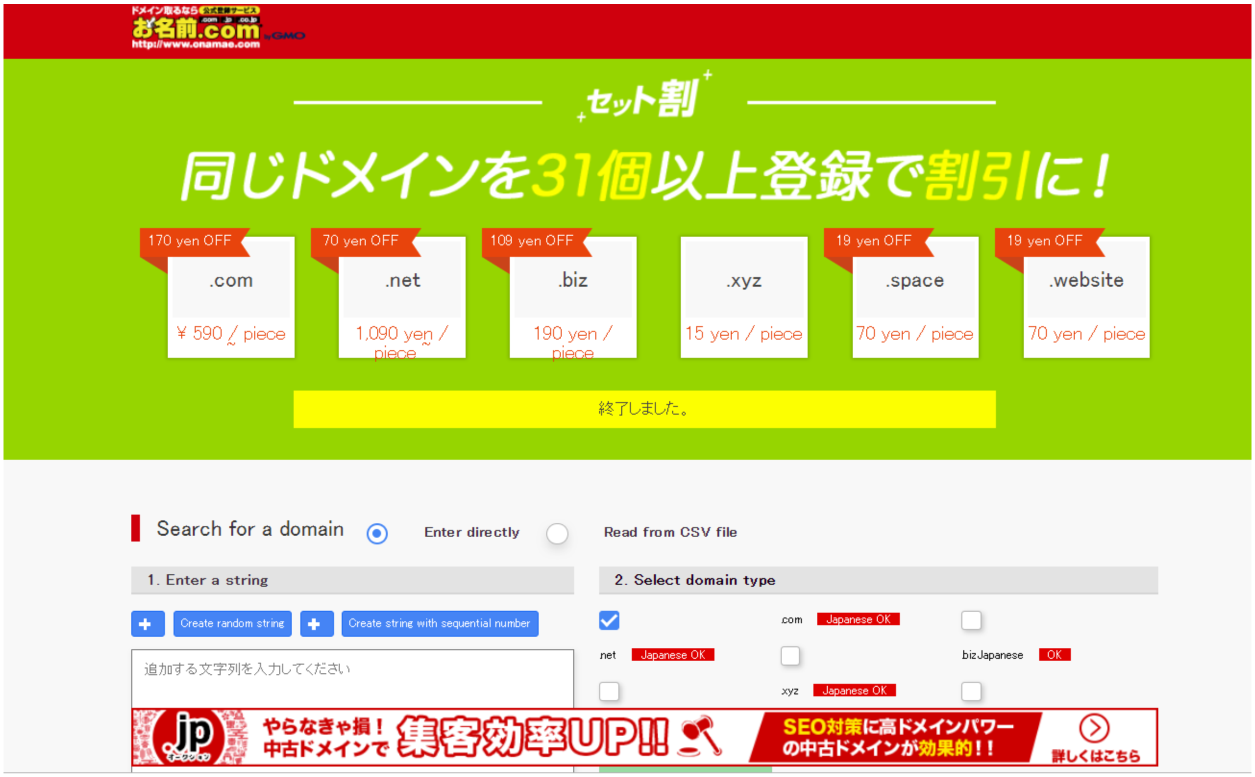


Chart 4: Creation dates of 6-character 2nd level labels in .TOKYO blocklisted domains

GMO Internet, Inc. offers "set discounts", which we interpret as volume or bulk registrations. They also offer a name generation form to create a random string or a string with sequential characters, as well. A translated copy of a “name creation” page illustrates the submission form and the most attractive pricing for several new gTLDs: notice that the form allows registrants to upload a file of names to register, or they can have strings automatically generated to compose a set of random-looking strings.



Search for a domain ● Enter directly ○ Read from CSV file

1. Enter a string

追加する文字列を入力してください

2. Select domain type

☑ .com Japanese OK □ .net Japanese OK □ .biz Japanese OK □ .xyz Japanese OK □

Figure 4: Screenshot of onamae.com bulk name registration methods (September 2019)

Registrars with high blocklist concentrations in .TOKYO

We used the Internet Archive Wayback Machine to obtain a copy of GMO Internet, Inc.’s registration page at onamae.com to learn that on February 18, 2018, a .TOKYO registration was priced at 99¥ or about $.92, an attractive price for acquiring attack or spam campaign resources in bulk.

At the time of writing this report, GMO was #3 on the Spamhaus Most Abused Registrars list. GMO Internet, Inc. has a long, recorded history as a registrar with a high concentration of domain names used in cyberattacks. We visited the Wayback Machine, where we determined that GMO was #3 on this list on February 9, 2017, #5 on October 18, 2018, and #5 on April 5, 2019.

Registrants responsible for high concentrations of blocklisted domains

Our .TOKYO sample spans a “post-GDPR” time period. GMO began redacting point of contact information for Whois records on May 25, 2018, and 8,564 Whois records of our sample of 8,715 blocked domains provided no registrant contact data. We *were* able to study complete Whois records for registrations that were collected prior to May 25, 2018 by a commercial service, Domain Tools.

We identified several registrant names from available and complete Whois records and investigated these using the Domain Tools IRIS and Seclytics Threat Intelligence systems. Using {registrant name, registrant organization, registrant email} individually or in combination, we were able to obtain additional intelligence for suspicious activities associated with one registrant.

Threat Intelligence obtained through search-and-pivot

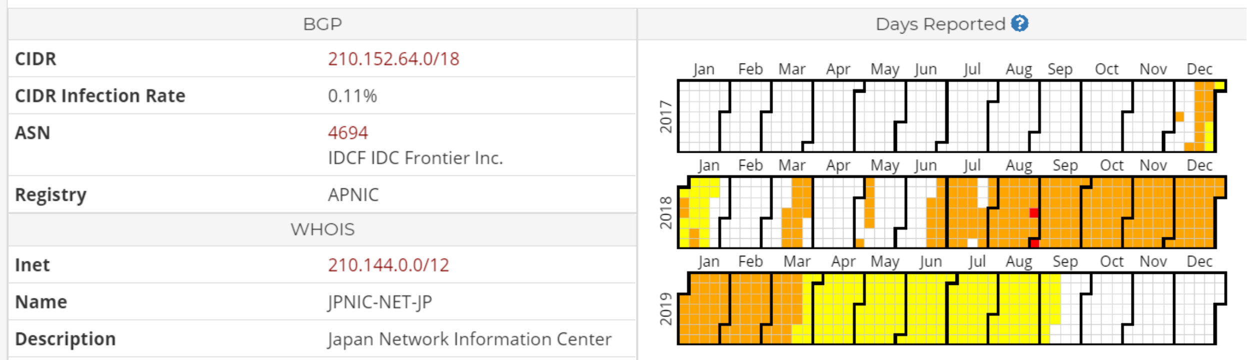
Using K◆n◆◆◆ T◆k◆◆◆◆◆◆[1] (registrant name) or T◆k◆◆◆◆◆◆ K◆n◆◆◆ (registrant organization) or ku◆◆◆◆12@yahoo.co.jp (registrant email) as search arguments, we found 282 domains containing one or more elements of this registrant's contact information in historical Whois databases. The registrant provided a contact address in Mie, Japan so is apparently not an EU data subject and thus not entitled to Europe's GDPR protection.

K◆n◆◆◆ T◆k◆◆◆◆◆◆ appears to exclusively register through GMO Internet., Inc. to direct malware, phishing attacks, or spam campaigns. We observed that the registrant did not focus exclusively on .TOKYO: we found elements of the registrant's POC in registrations from .BIZ, .CLUB, .INFO, .ONLINE, .SPACE, .WORK, and .XYZ.

We next used registrant name, email, and organization as arguments for searches into passive DNS, IP Whois, and other threat intelligence databases: this technique is called "search-and-pivot". The registrant K◆n◆◆◆ T◆k◆◆◆◆◆◆ appears to be familiar with and hosts servers at several hosting operators where criminal activities are known to be concentrated. To confirm this, we used passive DNS from Domain Tools IRIS to identify the IP addresses where registrant K◆n◆◆◆ T◆k◆◆◆◆◆◆ hosted services. We used the Seclytics attack prediction platform to obtain additional reputation data. We used heat maps generated by Seclytics to illustrate that the ASNs of the IP addresses used by the registrant exhibit high concentrations of a diverse set of security threats. Stop Forum Spam reports high spam activity at these ASNs (see ASN 7506 and ASN 131921).

Hostnames delegated from domain names blocklisted for phishing or malware (e.g., zfipotmet.TOKYO, hujiewai.TOKYO) were hosted at IP 210.152.84.234. This IP is assigned from 210.152.64.0/18, which is allocated under ASN 4096 to IDC Frontier, Inc.

Figure 5 shows a heat map of suspicious or criminal activity reported through Seclytics for this ASN. Heat maps use color as a data visualization tool. The Seclytics heat maps indicate the extent to which malicious or criminal misuse has been reported on a calendar date, from white (no reports) to deep red (many reports).



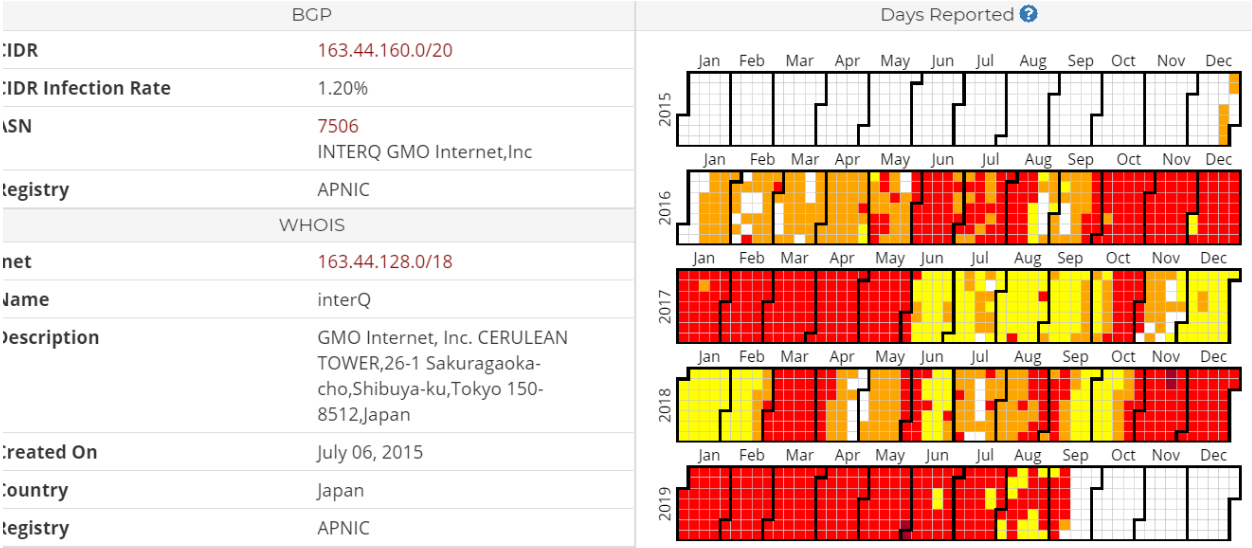
BGP	
CIDR	210.152.64.0/18
CIDR Infection Rate	0.11%
ASN	4694 IDCF IDC Frontier Inc.
Registry	APNIC
WHOIS	
Inet	210.144.0.0/12
Name	JPNIC-NET-JP
Description	Japan Network Information Center

Figure 5: Suspicious or criminal activity associated with ASN 4096 (IDC Frontier)

Hostnames delegated from domain names blocklisted for phishing or malware (e.g., acjprtd.TOKYO, aeiksainv.TOKYO) were hosted at IPs 163.44.170.118, assigned from 163.44.160.0/20, and 118.27.2.14,

[1] Names used in this report which could refer to real people have been obfuscated

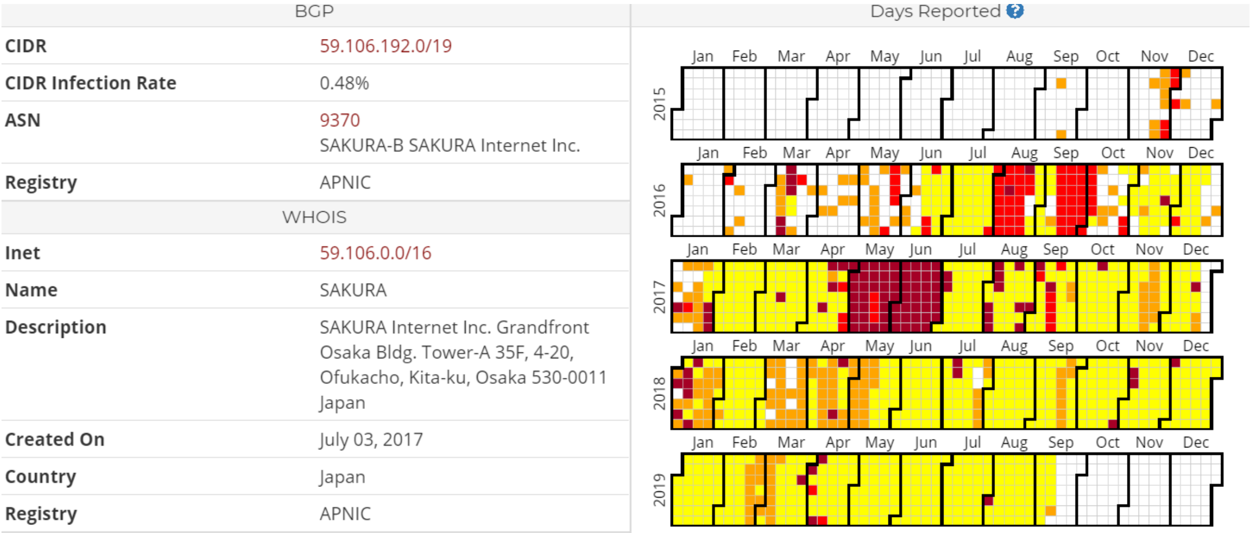
assigned from 118.27.2.0/20. These prefixes are allocated under ASN 7506 to INTERQ GMO Internet, Inc. Figure 6 shows a heat map of suspicious or criminal activity reported through Seclytics.



BGP	
IDR	163.44.160.0/20
IDR Infection Rate	1.20%
SN	7506 INTERQ GMO Internet,Inc
egistry	APNIC
WHOIS	
net	163.44.128.0/18
lame	interQ
escription	GMO Internet, Inc. CERULEAN TOWER,26-1 Sakuragaoka-cho,Shibuya-ku,Tokyo 150-8512,Japan
reated On	July 06, 2015
ountry	Japan
egistry	APNIC

Figure 6: Suspicious or criminal activity associated with ASN 7506 (INTERQ GMO Internet, Inc.)

Hostnames delegated from domain names blocklisted for phishing or malware (e.g., bnusiwu.TOKYO, yainegha.info) were hosted at IPs 59.106.208.237, assigned from 56.106.192.0/19, and 27.133.153.159, assigned from 27.133.128.0/19. These prefixes are allocated under ASN 9370 to SAKURA-B Internet, Inc. Figure 7 shows a heat map of suspicious or criminal activity reported through Seclytics.



BGP	
CIDR	59.106.192.0/19
CIDR Infection Rate	0.48%
ASN	9370 SAKURA-B SAKURA Internet Inc.
Registry	APNIC
WHOIS	
Inet	59.106.0.0/16
Name	SAKURA
Description	SAKURA Internet Inc. Grandfront Osaka Bldg. Tower-A 35F, 4-20, Ofukacho, Kita-ku, Osaka 530-0011 Japan
Created On	July 03, 2017
Country	Japan
Registry	APNIC

Figure 7: Suspicious or criminal activity associated with ASN 9370 (SAKURA-B Internet, Inc.)

Our study of .TOKYO illustrates the kinds of threat intelligence that investigators attempt to accumulate when complete Whois records are unavailable for all domains under investigation:

1. Our suspect composed random-looking domains when he registered in volume.
2. The suspect appears to have used GMO's bulk registration tools to generate names of the compositions we identified.

3. The suspect provided a registrant address in Japan.
4. GMO offered .TOKYO domains registrations at very low cost.
5. The domain names were identified as security threats and blocklisted by one or more reputation block list operators.
6. The suspect targeted .TOKYO but not exclusively. .INFO, .CLUB, .ONLINE, .XYZ, .BIZ, .SPACE, and .WORK were also targeted.
7. The suspect also took advantage of IP address space and ASNs that have histories of hosting multiple security threats.

Importantly, however, **our study of .TOKYO also illustrates what investigators can miss when Whois records are not available**, and how this affects the outcome of an investigation:

1. Registrations where contact data is redacted may also be associated with one of our suspects, but *we are unlikely to identify the registrant's full portfolio of domain names and hosting sites without access to contact data that is redacted by a registrar*.
2. Investigators have no contact data—in particular, names or email addresses—that they would typically use as potential search arguments or "handles", e.g., online aliases that they might use when they attempt to find a real world perpetrator by crossing over to social media platforms, Dark Web content, or other online content.
3. The criminal activity becomes more *survivable* in the face of partial detection: the domain names that investigators cannot find can allow the threat to persist while investigators wait for responses to requests to disclose non-public Whois information. In an October 2018 survey of the impact of ICANN's Temp Spec, "66% of responders report that their investigations have been affected since May 25, 2018: they have not found effective alternative data sources and their time to respond exceeds the acceptable threat threshold they, their organizations or local regulations prescribe."

Whether an investigator does this kind of analysis at the time of the event, or later, as a research or extended study, the inability to obtain complete Whois often yields a partial set of data or an incomplete map of the suspect's infrastructure. This may be true even when investigators have the original web site content or email messages. The investigator will be able to identify *some* of the domains used in possibly several attacks but perhaps not anywhere close to all domains used in any attack. Moreover, the investigator doesn't have sufficient data to take to a registrar or registry to suspend or seize a domain, nor do they have evidence sufficient to obtain a court order. And the criminal activity continues unabated.

Domain name misuse in .CLOUD

We studied blocklisting activity in .CLOUD from February 10, 2019 through February 13, 2019. Our sample set comprised 8,483 blocklisted domain names. At the time of this report, the Spamhaus badness index for .CLOUD was 26.4%, nearly seven times higher than for .COM (3.9%).

Registrars Targeted

Nearly all the blocklisted domains (99.8%) were registered through a single ICANN accredited registrar, GMO Internet, Inc. d/b/a Onamae.com, Inc. (the table omits registrars with a single blocklisted domain).

Registrar	IANA ID	Blocked Domains	Percent
GMO Internet, Inc. d/b/a Onamae.com	49	8,469	99.8
NameCheap, Inc.	1068	5	0.1
Tucows Domains Inc.	69	3	0.0

Table 3: Registrars with high concentrations of blocklisted domains in .CLOUD

Daily blocklisting activity

The sample in Chart 5 captures a significant blocklisting event: 8,281 of the 8,483 domains were blocklisted on February 12, 2019.

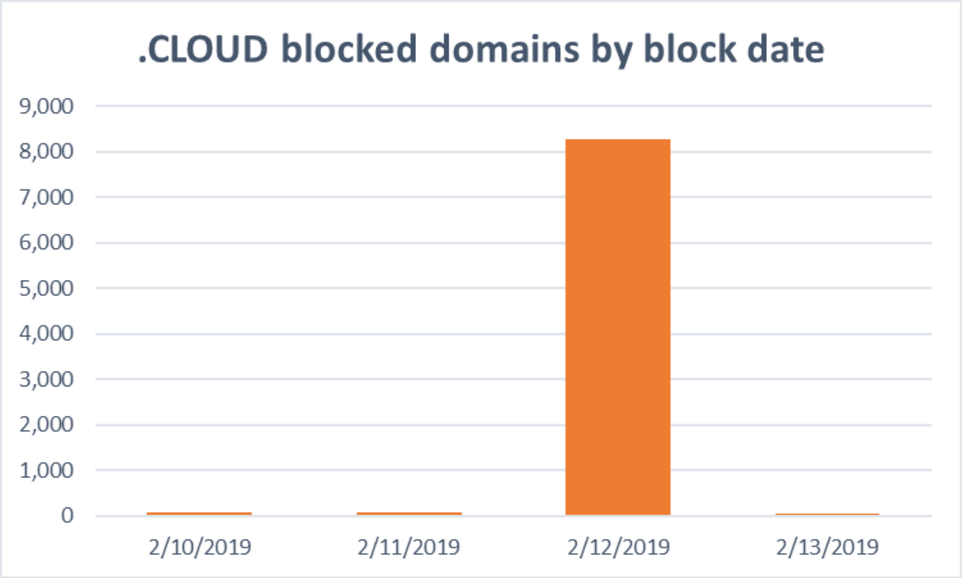


Chart 5: Earliest date of blocklisting of .CLOUD domains in sample

Blocking activity of the type we see on 2/12/2019 is indicative of a snowshoe spam campaign. The spammer registers a large number of domain names (over time), and later emits spam from mail exchanges that are hosted at many IPs or at hostnames delegated from the large pool of domains he has warehoused. By transmitting spam from mail relays from hundreds or thousands of senders, the spammer creates resiliency: investigators have to find *all* the domains to stop the attack.

Composition of 2nd level labels

The majority of blocklisted domains in this sample were between eight and seventeen characters long. We found no instances of labels containing recognizable English words: all of the 8,483 blocklisted domains in our sample exhibit patterns that are characteristic of random-looking domain names as previously described. This suggests that the registrants employed some auto-generation method.

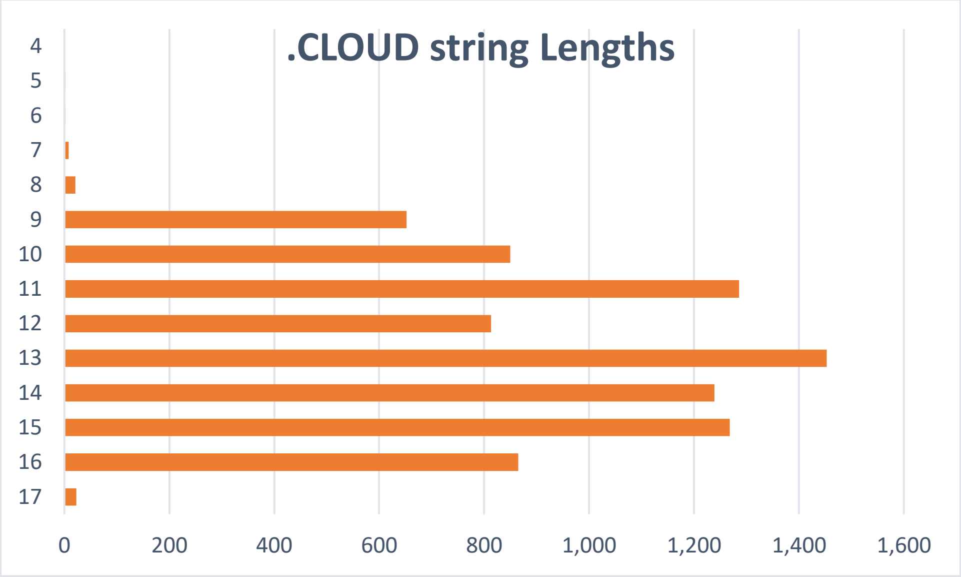


Chart 6: String lengths in .CLOUD blocklisted domains

Insights from creation date

The sample data reveals a pattern of creation dates that suggests some registrants repeatedly registered domain names in volume. Chart 7 shows that on eight different dates, approximately 1000 domains were registered that were ultimately blocklisted during the event we studied. We learned more by investigating registrants that had high concentrations of blocklisted domains in .CLOUD.

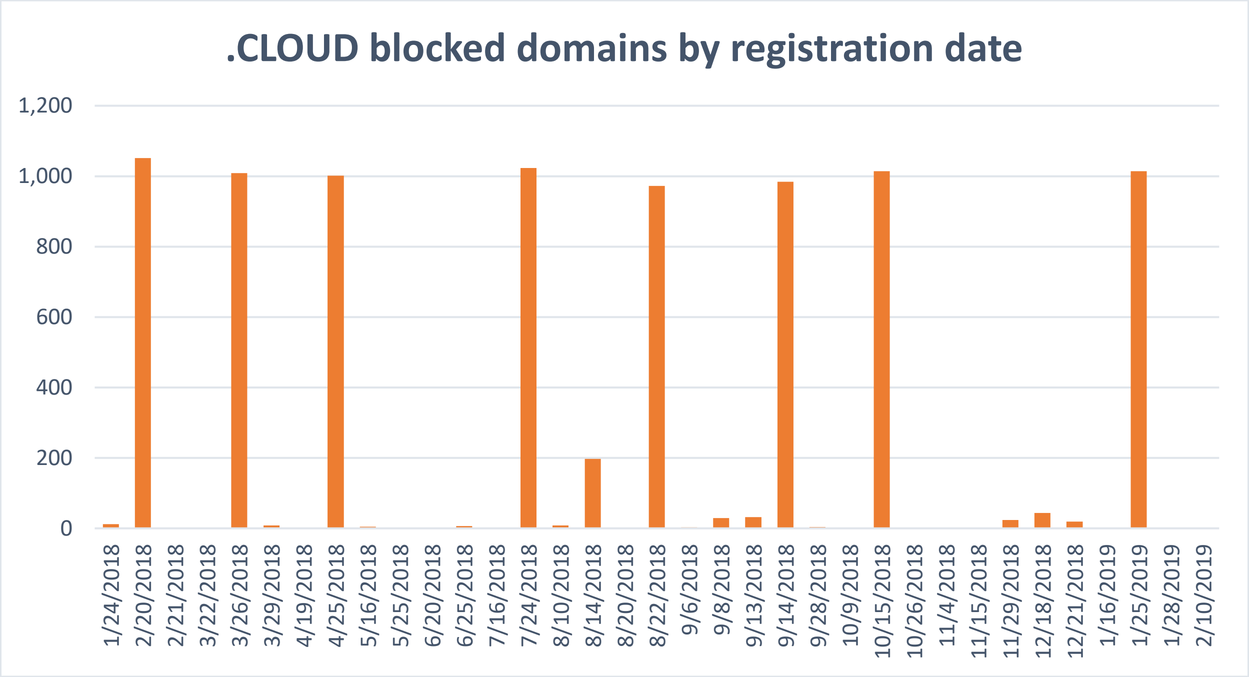


Chart 7: Blocklisted domains in .CLOUD, according to the domain creation date

Registrants responsible for high concentrations of blocklisted domains

Our .CLOUD sample again spans a “post-GDPR” time period. Registrant name was blank for 8,472 domain names in the sample. We *were* able to study the volume and registration behaviors of registrants by using available Registrant Organization values from domains that were registered prior to May 25, 2018. From available, complete Whois records, we observed that certain registrants would permute name strings; for example, we found Whois records where Registrant Organization is K◆◆k◆ T◆◆h◆◆◆◆◆ and Registrant Name is T◆◆h◆◆◆◆◆ K◆◆k◆. We observed the same behavior for the Registrant Organizations y◆◆s◆ t◆◆t◆◆◆◆ and S◆t◆◆◆ T◆k◆◆, and it is the same behavior we observed in .TOKYO (T◆k◆◆◆◆◆◆ K◆n◆◆◆).

Using the Domain Tools IRIS system, we were able to expand the search using the three values of Registrant Organization that had high concentrations of blocklisted domains:

Registrant Organization	Count	Percent
Whois Privacy Protection Service by onamae.com	5,148	60.7
y◆◆s◆ t◆◆t◆◆◆◆	1,049	12.4
K◆◆k◆ T◆◆h◆◆◆◆◆	1,009	11.9
S◆t◆◆◆ T◆k◆◆	998	11.8

Table 4: Registrants with high concentrations of blocklisted domains in CLOUD

Charts 8 and 9 illustrate that two of the Registrant Organizations, K◆◆k◆ T◆◆h◆◆◆◆◆ and S◆t◆◆◆ T◆k◆◆, registered domains in a “bulk manner” in .CLOUD:

- K◆◆k◆ T◆s◆◆h◆◆◆◆ registered *at* least 1007 domain names *in 33 minutes* and
- S◆t◆◆◆ T◆k◆◆ registered *at least* 996 domains *in 33 minutes* as well.

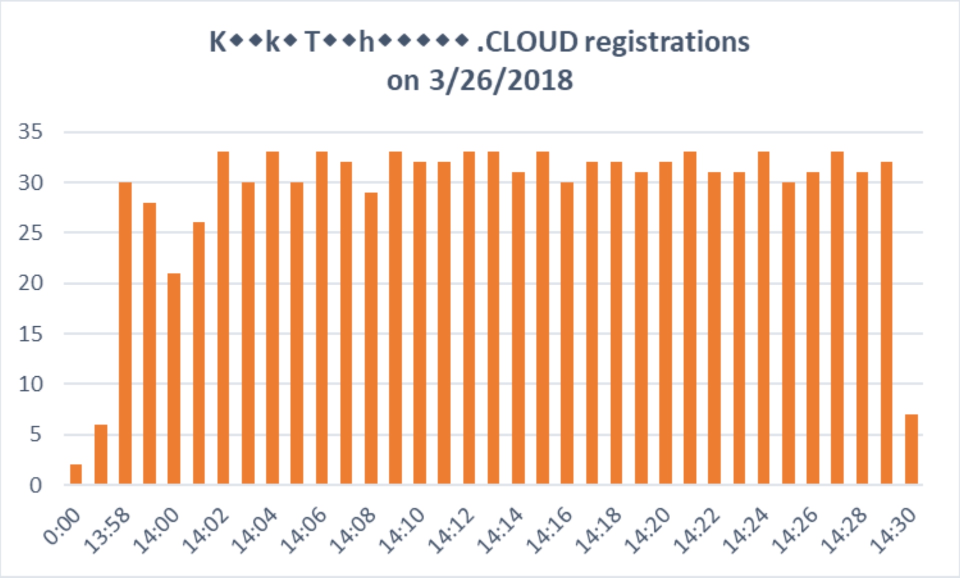


Chart 8: Rate of registration processing of Registrant Organization K◆◆k◆ T◆◆h◆◆◆◆◆

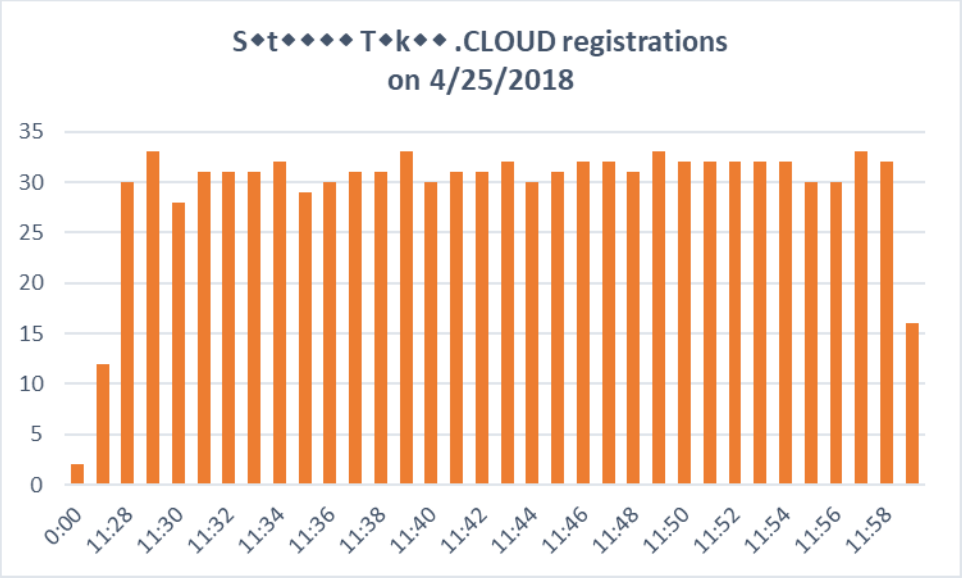


Chart 9: Rate of registration processing of Registrant Organization S◆t◆◆◆◆ T◆k◆◆

These charts only include the rates of registration behavior for .CLOUD domains that were in our sample and for which we found matches by searching on Registrant Organization. Domains that were registered in other TLDs and domains that were privacy protected are not included.

Timely and uniform access to complete Whois data records would allow investigators to search across collections of Whois records and map an attacker's domain or DNS infrastructure quickly. The benefit is obvious: upon confirmation that the suspicious behavior is a cybercrime or manifestation of a security threat, a near or complete set of domains associated with an attack can be blocklisted while the investigators request that a registrar or DNS hosting operator suspend name resolution for the attack domains, which would disrupt the attack and thus mitigate further harm or loss.

We next investigated suspects further using these names or other contact data as search arguments in and across several threat intelligence platforms.

Threat Intelligence obtained through search-and-pivot

Using the contact data of these three suspects, we queried the Domain Tools IRIS system. We were able to expand the search with Registrant Name and Registrant email address. We were able to obtain additional intelligence for suspicious activities associated with blocklisted domains in our sample:

Registrant Organization	Intelligence obtained through search-and-pivot
y◆◆s◆ t◆◆t◆◆◆◆	• 1,049 domains with Registrant Organization "y◆◆s◆ t◆◆t◆◆◆◆◆" also contained the "y◆◆s◆ t◆◆t◆◆◆◆◆" for Registrant Name and email is y◆◆s◆t◆t◆◆◆◆◆0◆◆0@gmail.com • The Registrant {City, Country} in these records is Tokyo, JP, indicating the registrant is likely a non-EU data subject. • All 1,049 domains were created on 2/20/2018
K◆◆k◆ T◆◆h◆◆◆◆◆◆	• 1,010 .CLOUD domains with Registrant Organization also contain the value "T◆◆h◆◆◆◆◆◆ K◆◆k◆" for Registrant Name and email is

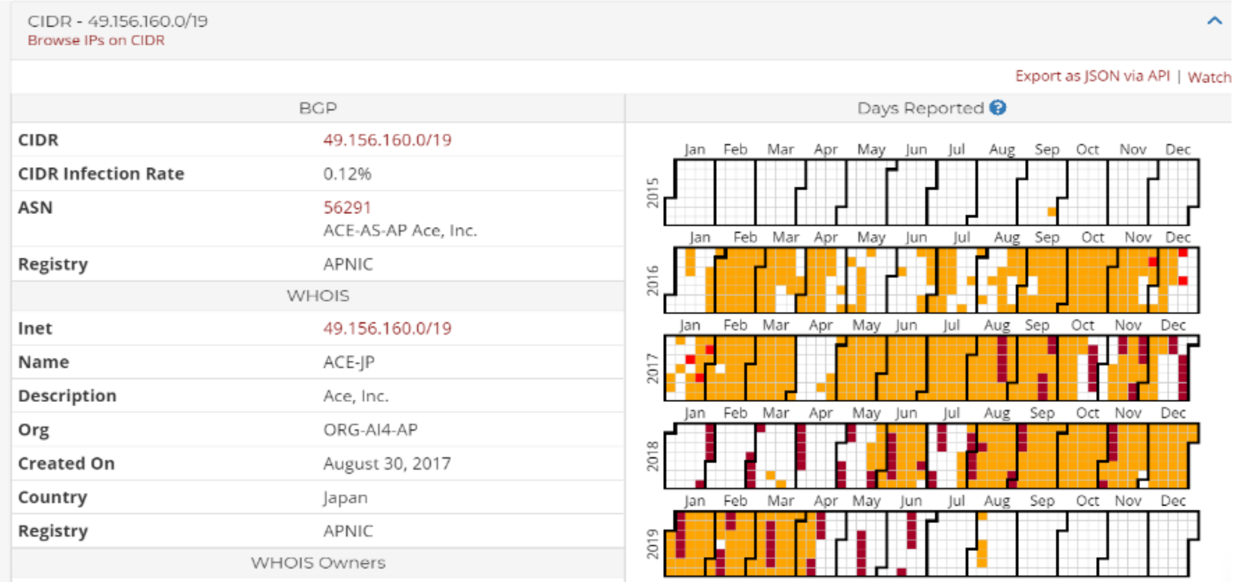
	n◆◆d◆◆◆1@gmail.com (Note: our expanded search identified one more than our .CLOUD data set contained) • The Registrant {City, Country} in these records is Tokyo, JP, indicating the registrant is likely a non-EU data subject • An additional 1,000 domains with these contact data are registered through GMO in .BIZ • All the domains were registered on 3/26/2018
S◆t◆◆◆ T◆k◆◆	• 1,049 domains with Registrant Organization "S◆t◆◆◆ T◆k◆◆" also contained "T◆k◆◆ S◆t◆◆◆" or "S◆t◆◆◆ T◆k◆◆" for Registrant Name and email is r◆d◆7◆o◆p◆@gmail.com • The Registrant {City, Country} in these records is Tokyo, JP, indicating the registrant is likely a non-EU data subject. • All 1,049 domains were created on 4/25/2018 • An additional 259 domains with these contact data are registered through GMO in .COM and 21 domains in .INFO

Table 5: Threat intelligence acquired by searching for Registrant Organization

Contact data reveals behaviors of known Japanese spammers

Our suspects appear to be familiar with and diversify across several hosting operators where criminal activities are known to be concentrated. We also observed some common hosting characteristics.

Naming convention similarities. Three persons of interest identified using the blocklisted domains in .CLOUD share a naming convention: all used the 3rd level label "mail" for presumably spam emitter hostnames (e.g., mail.abpbwmbnctfos.CLOUD, mail.zvroexmong.CLOUD). We found 537 of such assignments among S◆t◆◆◆ T◆k◆◆'s domains, 549 among K◆◆k◆ T◆◆h◆◆◆◆◆'s domains, and 325 among y◆◆s◆ t◆◆t◆◆◆◆'s domains.



CIDR - 49.156.160.0/19
Browse IPs on CIDR

Export as JSON via API | Watch

BGP	
CIDR	49.156.160.0/19
CIDR Infection Rate	0.12%
ASN	56291 ACE-AS-AP Ace, Inc.
Registry	APNIC
WHOIS	
Inet	49.156.160.0/19
Name	ACE-JP
Description	Ace, Inc.
Org	ORG-AI4-AP
Created On	August 30, 2017
Country	Japan
Registry	APNIC
WHOIS Owners	

Figure 8: Heat map of 49.156.160.0/19, in ASN 56291 – ACE-AS-AP Ace, Inc.

Common hosting operations. All these hostnames resolved to an IP address within the CIDR block 49.156.160.0/19. This CIDR block is assigned to ACE-AS-AP Ace, Inc. and is announced in ASN 56291. A Seclytics heat map in Figure 8 illustrates that this ASN has a long history of IP addresses used in spam campaigns or to manifest other security threats:

Known spam gang operations. Spamhaus has listed this address block on its Spamhaus Block List (SBL 169202) as "being assigned to, being under the control of, or being otherwise connected with a known spam operation listed on the ROKSO database". The "known spammer" on the ROKSO (Register Of Known Spam Operators) is pur. Interestingly, Spamhaus created SBL 169202 on February 19, 2018: that date corresponds to the first bulk registration spike in Chart 7. Other IP address blocks that the spammers used for hosting "www" hostnames are also on the SBL, including:

IP block	SBL	Registrant	Used for
103.205.10.0/24	SBL320958	K◆◆k◆ T◆◆h◆◆◆◆◆, S◆t◆◆◆ T◆k◆◆, y◆◆s◆ t◆◆t◆◆◆◆	malware hostnames of the form www.<random-looking-string>CLOUD
113.212.143.0/19	SBL78429	K◆◆k◆ T◆◆h◆◆◆◆◆, S◆t◆◆◆ T◆k◆◆	malware hostnames of the form www.<random-looking-string> .BIZ Name server hosting
111.223.192.0/19	SBL78432	y◆◆s◆ t◆◆t◆◆◆◆	Name server hosting

Table 6: Three persons of interest host their attack services on IP prefixes enumerated on the Spamhaus Block List

Our study of .CLOUD demonstrates what investigators can learn when complete Whois records are available. In this case, we were able to determine that

1. Multiple suspects appear to have used GMO Internet Inc.'s bulk registration service to acquire approximately 1,000 or more domain names in a matter of minutes.
2. The registrar has a history of offering attractive pricing for domain registrations, especially among the new gTLDs. At the time of writing this report, GMO was offering .CLOUD registrations for 199 ¥ (under $2.00 US), .WORK and .XYZ registrations for 1 ¥, and .SITE registrations for 60 ¥. The Wayback Machine web archives also show low pricing for registrations throughout 2018.
3. The suspects share a common practice: they permute name strings when they submit registration data for Registrant Organization and Registrant Name. We observed this in one registrant in our .TOKYO sample as well.
4. The suspects provided a registrant address in Japan.
5. The suspects compose random-looking domains when they register in volume. The registrar, GMO Internet, Inc., provides a name suggestion tool that can generate names of the composition we identified.
6. The domain names were identified as security threats and blocklisted by one or more reputation block list operators.
7. The suspects targeted .CLOUD but not exclusively. Both .BIZ and .INFO were also targeted.
8. The suspects also took advantage of IP address space and ASNs that have histories of hosting multiple security threats.
9. The suspects' behaviors match the patterns that Spamhaus attributes to organized Japanese spam gangs.

Domain name misuse in .XYZ

We studied blocklisting activity in XYZ from February 17, 2018 through February 21, 2018. After filtering incomplete records, we reduced our sample to 9,155 domain names. At the time of this report, the Spamhaus badness index for XYZ was 8.9%, more than double that of COM (3.9%).

Registrars with high blocklist concentrations in .XYZ

Four registrars account for 93% of the blocklisted domain names in .XYZ in our sample. We found the highest concentration of blocklisted registrations at GMO Internet, Inc.

Registrar	IANA ID	Blocked Domains	Percent
GMO Internet, Inc. d/b/a Onamae.com	49	8,035	87.8
Hostinger, UAB	1636	196	2.1
PDR Ltd. d/b/a PublicDomainRegistry.com	303	193	2.1
GoDaddy.com, LLC	146	104	1.1

Table 7: Registrars with high blocklist concentrations in .XYZ

Daily blocklisting activity

The sample in Chart 10 captures a significant blocklisting event: 8,139 of the 9,155 domains were blocklisted on February 20, 2019.

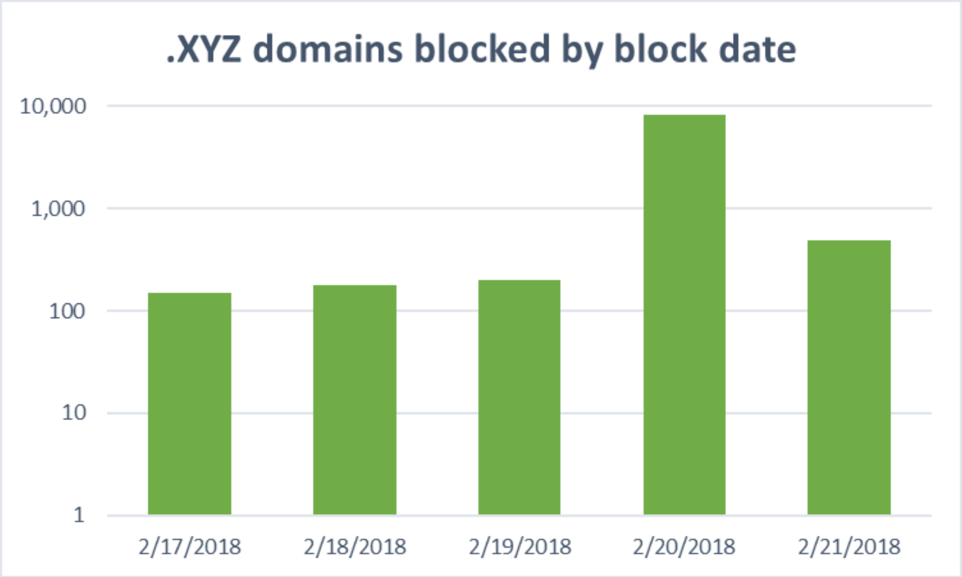


Chart 10: Daily blocklisting activity in .XYZ (Note—this chart uses a logarithmic scale)

Blocklisting activity of the type illustrated for 2/20/2018 is often indicative of snowshoe spam campaign activity, where the spammer attempts to thwart detection by emitting spam from mail exchanges that are hosted at many IPs or at hostnames delegated from a large number of domain names, all registered to a common registrant.

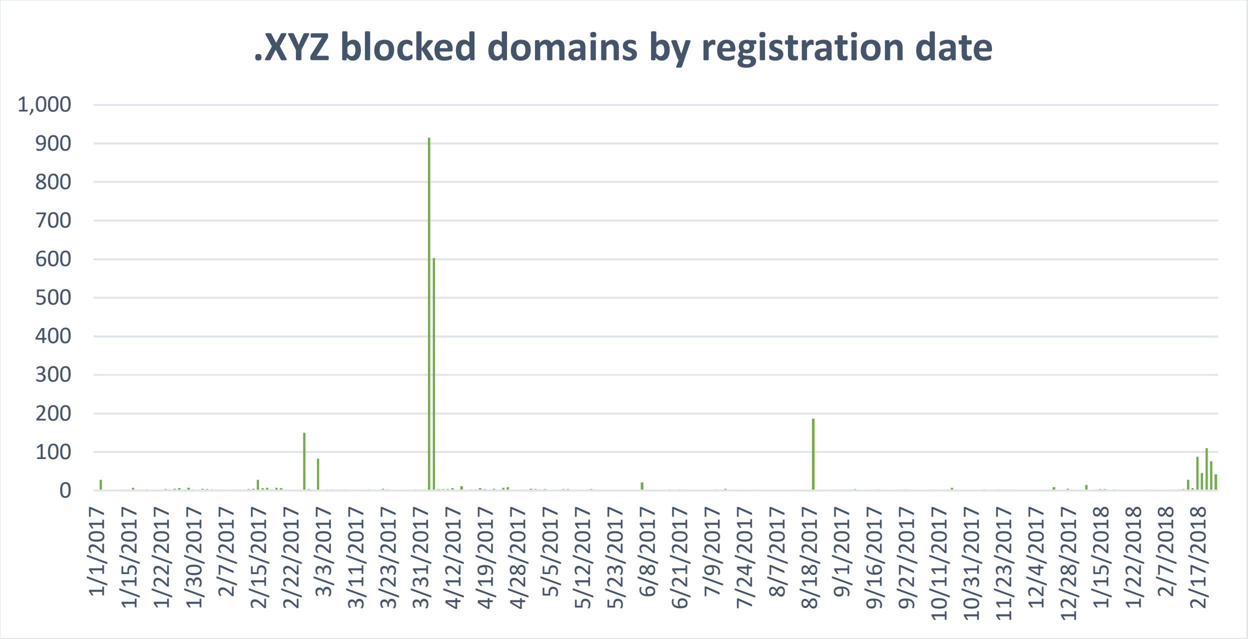


Chart 11: Blocklisting activity in .XYZ by registration date

Composition of 2nd level labels

This sample set has both random-looking strings, with or without hyphens (e.g., l6bu8jbjxyj.XYZ, ortfnu-eiauad.XYZ), and strings that consist of or contain one or more English words (landwatch.XYZ, myworkmustpayme.XYZ, zyxonline.XYZ, or willow-scourge.XYZ). Many patterns and lengths appear. These could plausibly have been created using GMO's name generation tool or they could have been uploaded as a csv file.

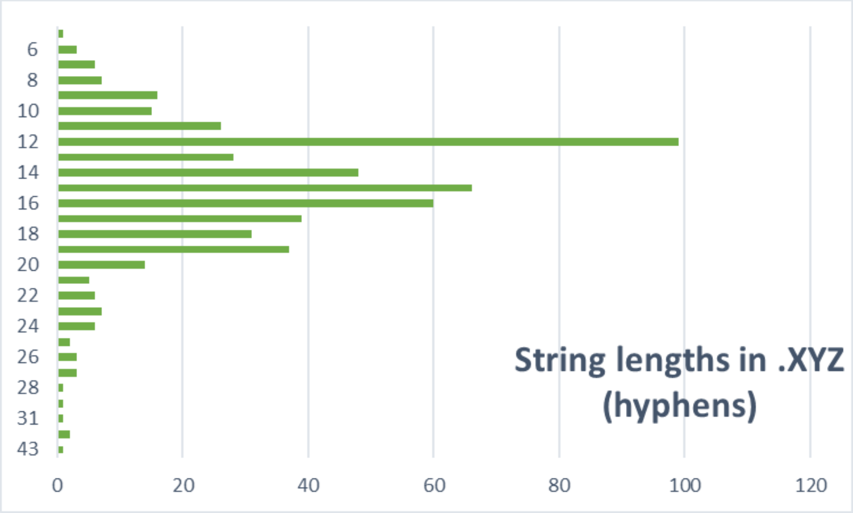


Chart 12: String lengths in .XYZ with hyphens

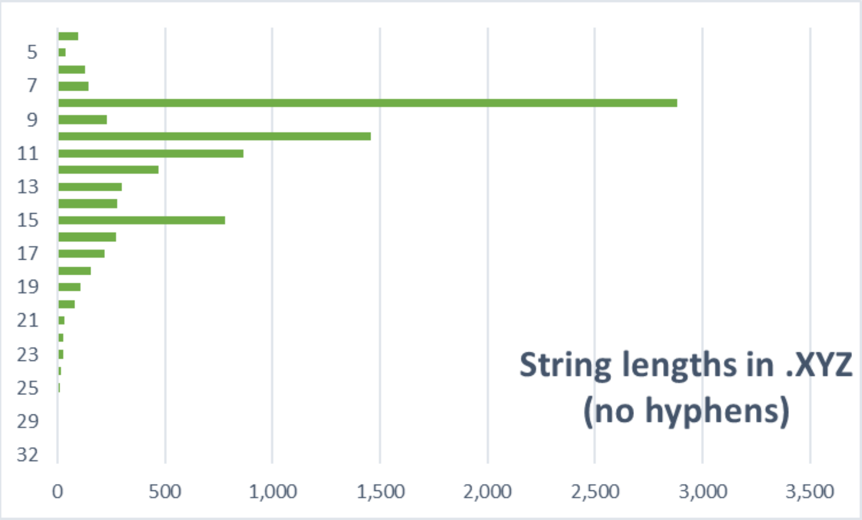


Chart 13: String lengths in .XYZ without hyphens

Registrants responsible for high concentrations of blocklisted domains

Three registrants are responsible for high concentrations of blocklisted domains. We note that two registrants again permute the name strings in Registrant Name and Registrant Organization.

Registrant Name	Domain Count	Percent	Registrant Organization	Registrant Email
T◆d◆s◆i K◆n◆m◆t◆	959	10.5	T◆d◆s◆i K◆n◆m◆t◆	arithmetic19750824@yahoo.co.jp
D◆i◆i K◆m◆t◆u	877	9.6	D◆i◆i K◆m◆t◆u	mail@xxx.angel-of-xxx.com
T◆r◆k◆ A◆a◆k◆	830	9.1	T◆r◆k◆ A◆a◆k◆	phenomenon77777@yahoo.co.jp

Table 8: Registrants with high concentrations of blocklisted domains in our .XYZ blocklist sample

Threat Intelligence obtained through search-and-pivot

When complete Whois records are available, researchers can do deep historical studies. For example, we found that Registrant contact data in Table 8 for T◆d◆s◆i K◆n◆m◆t◆ appears in 6,672 available Whois records dating back to 2002 (Note that in some historical Whois records, the registrant used “Personal” in the Registration Organization field, as well.)

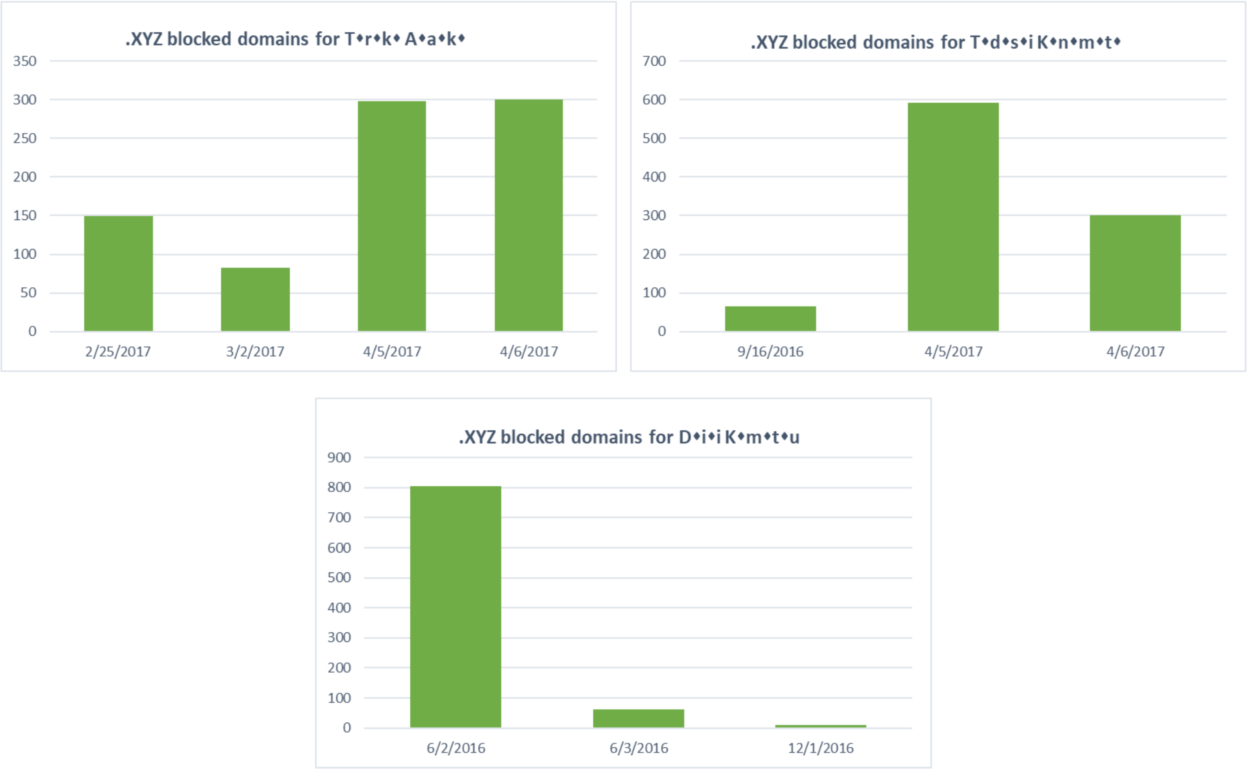
T◆d◆s◆i K◆n◆m◆t◆ registered 47% of his “portfolio” in .COM, .NET and the .PW and .JP ccTLD. The other 53% were registered across the new TLD delegations.

TLD	Domains	TLD	Domains
accountant	100	net	1,741
click	250	pw	29
club	500	shop	1,171
com	1,249	tokyo	5
cricket	100	top	1
jp	45	work	32
nagoya	5	xyz	1,404
		yokohama	40
Grand Total 6,672			

In addition to 1,404 Whois records we found for domains delegated from .XYZ, we also found 5,268 domains registered across the gTLD space. The reputation scoring available from our threat intelligence tools indicates that the domains under this registrant's management have historically scored poorly: they are either classified as phishing, malware, or spam, or they were marked suspicious (e.g., factors such as common IP address, creation date, name server, along with common contact data all contribute to a high risk score).

We note that with complete Whois records, investigators or blocklist operators could take pre-emptive actions should the registrant continue to use this account. When Whois is redacted, and timely access to contact data is unavailable, investigators work harder and longer, and the windows of opportunity for attacks are extended.

Our thee suspect registrants all appear to have used some form of bulk registration automation. Of the domains we could find, T◆r◆k◆ A◆a◆k◆ (Chart 14, left, below) registered approximately 300 domains on April 5, 2018 and April 6, 2018. T◆d◆s◆i K◆n◆m◆t◆ registered 593 domains on April 5 and 300 on April 6 (Chart 15, right, below). Of the 877 domains we associated with D◆i◆i K◆m◆t◆u, 806 were registered on June 2, 2016 (Chart 16, bottom, below).



Charts 14, 15, and 16: bulk registrations of T◆r◆k◆ A◆a◆k◆ (Upper left), T◆d◆s◆i K◆n◆m◆t◆ (Upper right) and D◆i◆i K◆m◆t◆u (bottom)

Registrant Contact data (name, organization, or email) for D◆i◆i K◆m◆t◆u appears in 13,010 of the Whois records that we can access. We found several common data points between this registrant and T◆d◆s◆i K◆n◆m◆t◆:

- Registrations in .XYZ, .CLICK, .CLUB, .WORK, .TOKYO, .COM, .YOKAHAMA, .TOP, and. SHOP (also in .LINK, .BIZ, .ORG, .ME, .PW, .CO)
- Hostnames containing "mail" in 49.156.170.0/19 ASN 56291 "ACE-AS-AP Ace, Inc."

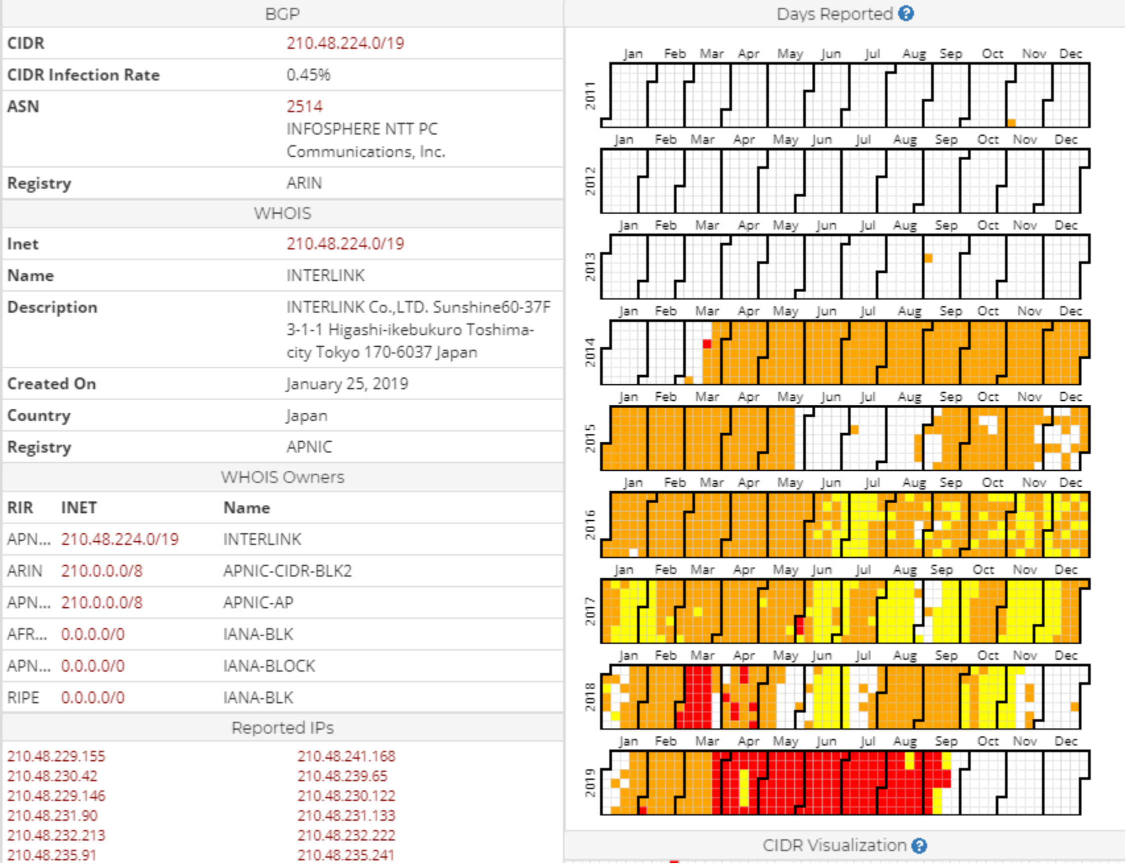
- Hosting in 113.212.143.73 ASN 56291 “ACE-AS-AP Ace, Inc.”

Registrant Contact data (name, organization, or email) for T◆r◆k◆ A◆a◆k◆ appears in 5,451 of the Whois records that we can access. We find several common data points between this registrant and T◆d◆s◆i K◆n◆m◆t◆ as well:

- Registrations in .XYZ, .CLUB, .WORK, .COM, .YOKAHAMA, .PW, and .TOKYO (also in .NET, .WIN, .ME, .PW, and .SHOP)
- Hostnames containing “mail” in 49.156.170.0/19 ASN 56291 “ACE-AS-AP Ace, Inc.”
- Hosting in 113.212.143.73 ASN 56291 “ACE-AS-AP Ace, Inc.”

More Japanese Spammers

As we observed from our .CLOUD sample, we once again see “mail” hostnames hosted at IP addresses within the CIDR block 49.156.160.0/19, advertised using ASN 56291 “ACE-AS-AP Ace, Inc.,” which we have previously identified as a known locus for spammers. We found 1,064 such hostnames assigned to 49.156.170.245 and 974 to 49.156.179.240. We also see mail hostnames assigned to IP addresses in 210.48.240.0/19, ASN 2514 “INFOSPHERE NTT PC Communications, Inc.,” and 111.223.196.0/19, ASN 56291 “ACE-AS-AP Ace, Inc.,” which we previously identified from Spamhaus SBL78432 as part of the *pur* spam operation. This registrant appears to be another Japanese spammer account, possibly related to or conspiring with those we identified from our study of .CLOUD.



BGP	
CIDR	210.48.224.0/19
CIDR Infection Rate	0.45%
ASN	2514 INFOSPHERE NTT PC Communications, Inc.
Registry	ARIN
WHOIS	
Inet	210.48.224.0/19
Name	INTERLINK
Description	INTERLINK Co.,LTD. Sunshine60-37F 3-1-1 Higashi-ikebukuro Toshima-city Tokyo 170-6037 Japan
Created On	January 25, 2019
Country	Japan
Registry	APNIC

WHOIS Owners

RIR	INET	Name
APN...	210.48.224.0/19	INTERLINK
ARIN	210.0.0.0/8	APNIC-CIDR-BLK2
APN...	210.0.0.0/8	APNIC-AP
AFR...	0.0.0.0/0	IANA-BLK
APN...	0.0.0.0/0	IANA-BLOCK
RIPE	0.0.0.0/0	IANA-BLK

Reported IPs

210.48.229.155	210.48.241.168
210.48.230.42	210.48.239.65
210.48.229.146	210.48.230.122
210.48.231.90	210.48.231.133
210.48.232.213	210.48.232.222
210.48.235.91	210.48.235.241

Days Reported

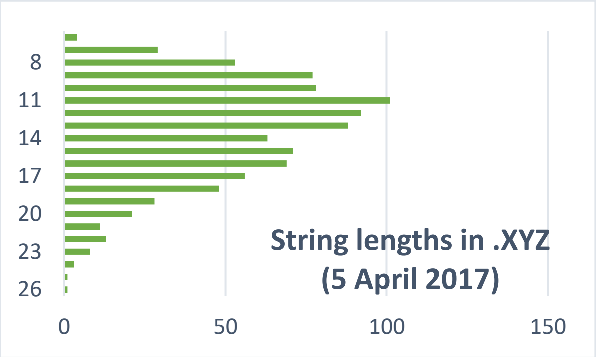
CIDR Visualization

Figure 9: Suspicious or criminal activity associated with ASN 2514 (INFOSPHERE NTT PC)

The .XYZ sample shows one significant registration (creation date) event—refer to Chart 11, earlier.

We observed several interesting patterns on April 5, 2017.

- The triplet {K◆n◆k◆ H◆r◆h◆r◆, K◆n◆k◆ H◆r◆h◆r◆, j◆u◆c◆a◆1◆3◆8◆@yahoo.co.jp} registered 24 two-word names
- The triplet {T◆d◆s◆i K◆n◆m◆t◆, K◆n◆m◆t◆ T◆d◆s◆i, arithmetic19750824@yahoo.co.jp} registered 593 two-word domains
- The triplet {T◆r◆k◆ A◆a◆k◆, A◆a◆k◆ T◆r◆k◆, phenomenon77777@yahoo.co.jp} registered 298 two-word domains



As part of a deeper investigation, investigators might pursue the theory that these accounts, perhaps along with suspect registrants we studied in the .TOKYO and .CLOUD samples, are related; e.g., the registrants were working together on that day (a conspiracy), or (assuming these are fraudulently composed) the same individual was using multiple accounts to enhance his deception.

In summary, with access to complete Whois records, we were able to determine that

1. Multiple suspects again extensively used GMO Internet, Inc., to acquire attack domain names.
2. The suspects composed random-looking domains when they registered in volume.
3. XYZ is one of several new gTLDs that GMO Internet, Inc. offers for low registration fees.
4. As we observed in our .TOKYO and .CLOUD samples, suspects again permuted name strings when they submitted registration data for Registrant Organization and Registrant Name.
5. The domain names were identified as security threats and blocklisted by one or more reputation block list operators.
6. The suspects targeted .XYZ but not exclusively. The Whois contact data associated with domains in our .XYZ sample helped us search and locate thousands of domains registered by three subjects in over twenty (20) ccTLDs and gTLDs.
7. The suspects also took advantage of IP address space and ASNs that have histories of hosting multiple security threats.
8. The suspects' choices of hosting operators match the patterns that Spamhaus attribute to organized Japanese spam gangs.

Few of these associations are possible when Whois contact data is not available.

Domain name misuse in .TOP

We studied blocklisting activity in a sample of 163,148 domain names from .TOP from February 2, 2018 through February 28, 2018. At the time of this report, the Spamhaus badness index for .COM is 3.9%. .TOP's 31.8% badness index is nearly 9 times larger.

We also studied a sample of 166,081 domain names from October 19, 2018 through October 31, 2018. This allows us to compare and contrast samples where complete Whois records were available for all domains in the set against a sample where a large percentage of Whois records were redacted for privacy.

Registrars with high blocklist concentrations in .TOP

Five registrars account for 95% of the blocklisted domain names in .TOP in our February 2018 sample.

Registrar	IANA ID	Blocked Domains	Percentage
Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	1599	103,179	63.2
Alpnames Limited	1857	24,345	14.9
GMO Internet, Inc. d/b/a Onamae.com	49	16,071	9.9
Chengdu West Dimension Digital Technology Co., Ltd.	1556	7,771	4.8
PDR Ltd. d/b/a PublicDomainRegistry.com	303	2,901	1.8

Table 9: Registrars with high concentrations of blocklisted domains in our .TOP sample, February 2018

In the February 2018 sample, Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn) has the highest concentration of blocklisted domains with 103,179.

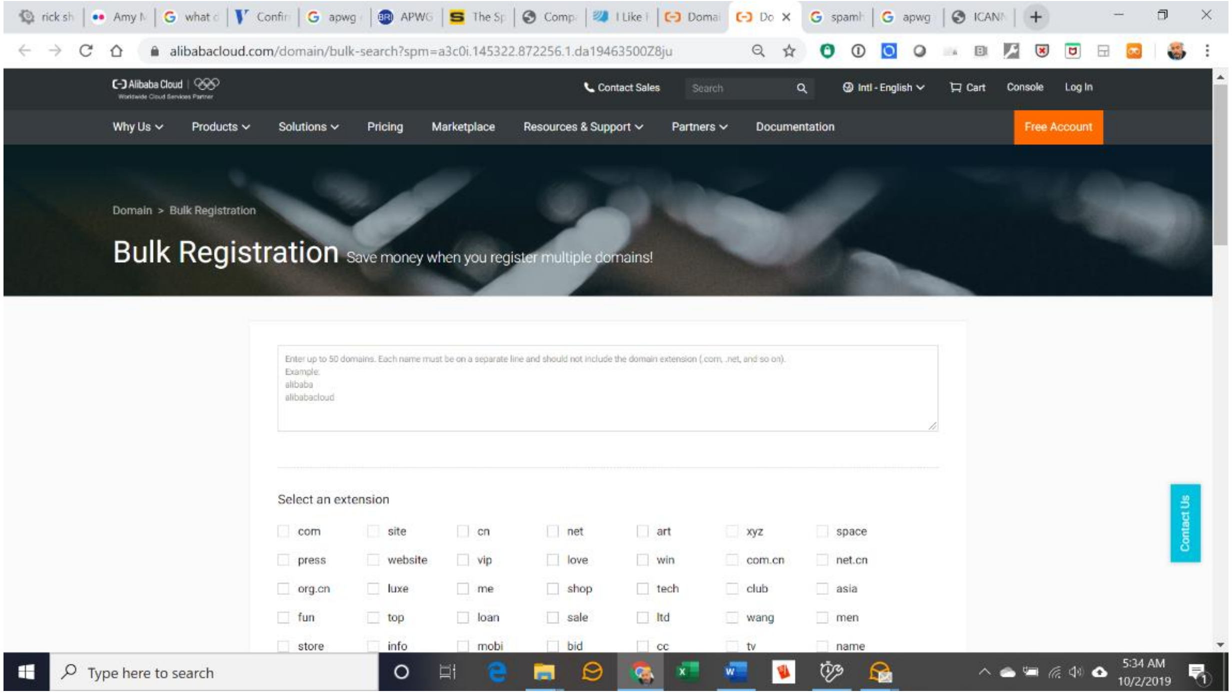
Registrar	IANA ID	Blocked Domains	Percentage
Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	1599	55,714	33.5
Chengdu West Dimension Digital Technology Co., Ltd.	1556	37,292	22.5
Alpnames Limited	1857	35,295	21.3
GMO Internet, Inc. d/b/a Onamae.com	49	10,618	6.4
PDR Ltd. d/b/a PublicDomainRegistry.com	303	9,057	5.5

Table 10: Registrars with high concentrations of blocklisted domains in our .TOP sample, October 2018

In the October 2018 sample, HiChina remains the registrar with the highest concentration of blocklisted domains (55,714), but Chengdu West (37,292) and Alpnames Limited also have high concentrations of blocklisted domains (35,295).

In both samples, Asia-Pacific registrars hold dominant percentages of the total blocklisted domains.

Alibaba Cloud Computing (HiChina) offers a bulk registration service (Figure 10). A customer can submit fifty domains through the web form, place these in a shopping cart, and repeat the process.



Domain > Bulk Registration

Bulk Registration Save money when you register multiple domains!

Enter up to 50 domains. Each name must be on a separate line and should not include the domain extension (.com, .net, and so on).
Example:
alibaba
alibabacloud

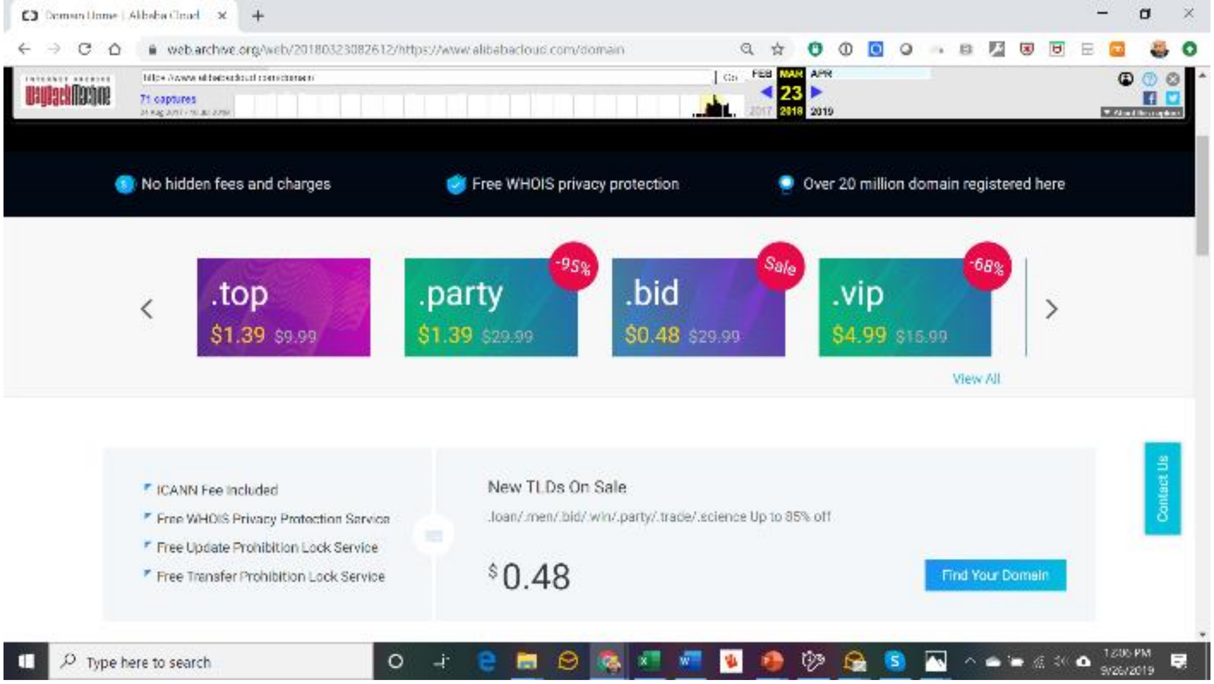
Select an extension

□ com	□ site	□ cn	□ net	□ art	□ xyz	□ space
□ press	□ website	□ vip	□ love	□ win	□ com.cn	□ net.cn
□ org.cn	□ luxe	□ me	□ shop	□ tech	□ club	□ asia
□ fun	□ top	□ loan	□ sale	□ ltd	□ wang	□ men
□ store	□ info	□ mobi	□ bid	□ cc	□ tv	□ name

Figure 10: Alibaba Bulk Registration web form

From the Wayback Machine we find a February 13, 2018 archive of the domain search page (Figure 11).

Comparing this against a page captured on September 26, 2019 (see Figure 12), we observe that .TOP and other new gTLDs are attractively priced.



No hidden fees and charges

Free WHOIS privacy protection

Over 20 million domain registered here

.top	.party	.bid	.vip
$1.39 $9.99	-95% $1.39 $29.99	Sale $0.48 $29.99	-68% $4.99 $15.99

View All

- ICANN Fee Included
- Free WHOIS Privacy Protection Service
- Free Update Prohibition Lock Service
- Free Transfer Prohibition Lock Service

New TLDs On Sale

.loan/.men/.bid/.win/.party/.trade/.science Up to 85% off

$0.48

Find Your Domain

Domain Home | Alibaba Cloud
web.archive.org/web/20180323082612/https://www.alibabacloud.com/domain
71 captures
FEB MAR APR
23
2017 2018 2019
Contact Us
Type here to search
9/26/2019

Figure 11: .TOP domain pricing at Alibaba Cloud Computing, Ltd., February 2018

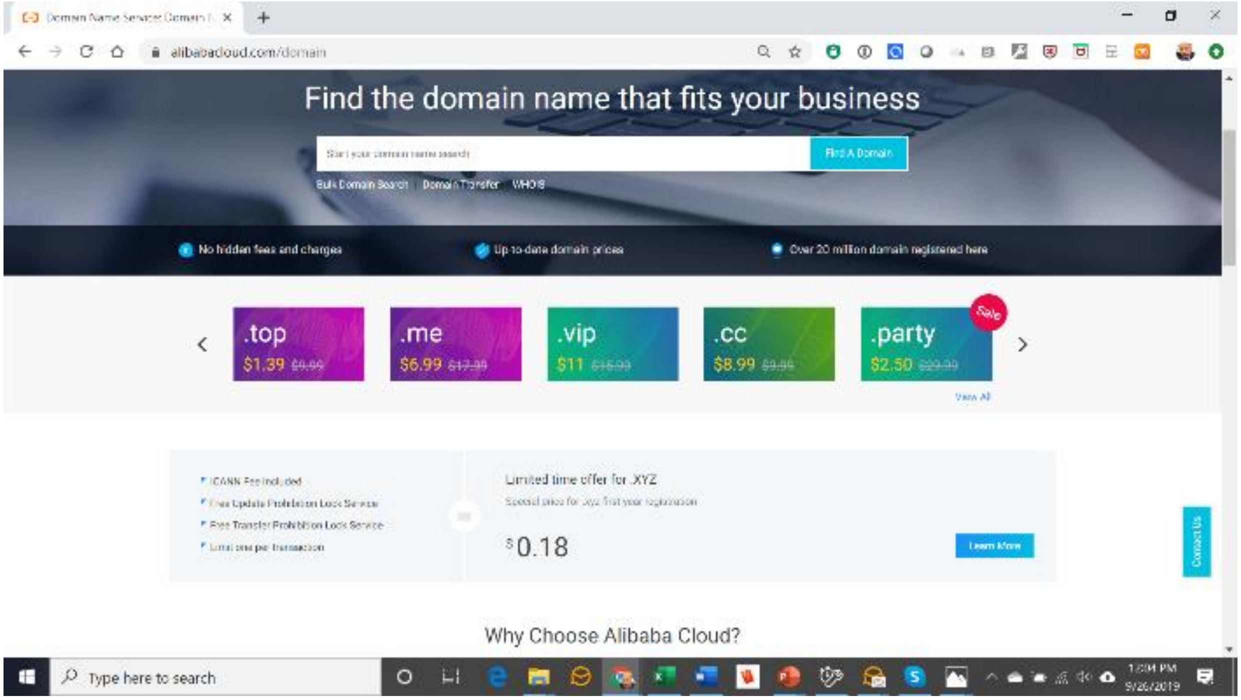

Domain Name Service: Domain N
alibabacloud.com/domain
Find the domain name that fits your business
Start your domain name search
Find A Domain
Bulk Domain Search | Domain Transfer | WHOIS
No hidden fees and charges
Up-to-date domain prices
Over 20 million domain registered here
.top $1.39 ~~$9.99~~
.me $6.99 ~~$17.99~~
.vip $11 ~~$16.99~~
.cc $8.99 ~~$9.99~~
.party $2.50 ~~$29.99~~
Sale
View All
ICANN Fee Included
Free Update Prohibition Lock Service
Free Transfer Prohibition Lock Service
Limit one per transaction
Limited time offer for .XYZ
Special price for .xyz first year registration
$0.18
Learn More
Contact Us
Why Choose Alibaba Cloud?
Type here to search
1:34 PM
9/26/2019

Figure 12: .TOP domain pricing at Alibaba Cloud Computing, Ltd., September 2019

Registrar Notoriety

In the October 2018 sample, HiChina again has the highest concentration of blocklisted domains with 55,714 but only 33% of the 166,081 domains in the sample. Chengdu West Dimension Digital Technology has a large share of registrations of new TLDs. Chengdu West Dimension Digital Technology Co., Ltd. was ranked 8th in Domain Tools' 2016 Report, The Distribution of Malicious Domains, and AlpNames was ranked 3rd. ICANN terminated its Registrar Accreditation Agreement with AlpNames in March 2019. Prior to March 2019, AlpNames was a notorious "penny domain" registrar. In May 2018, technology companies demanded that ICANN Compliance investigate AlpNames, citing the ICANN-commissioned August 2017 Statistical Analysis of DNS Abuse in gTLDs, which associated AlpNames with over one-half of the blocklisted domains in the new TLD program.

Daily blocklisting activity

In both the February and October 2018 samples, we see extraordinary numbers and frequency of dates where thousands of domains were blocklisted daily.

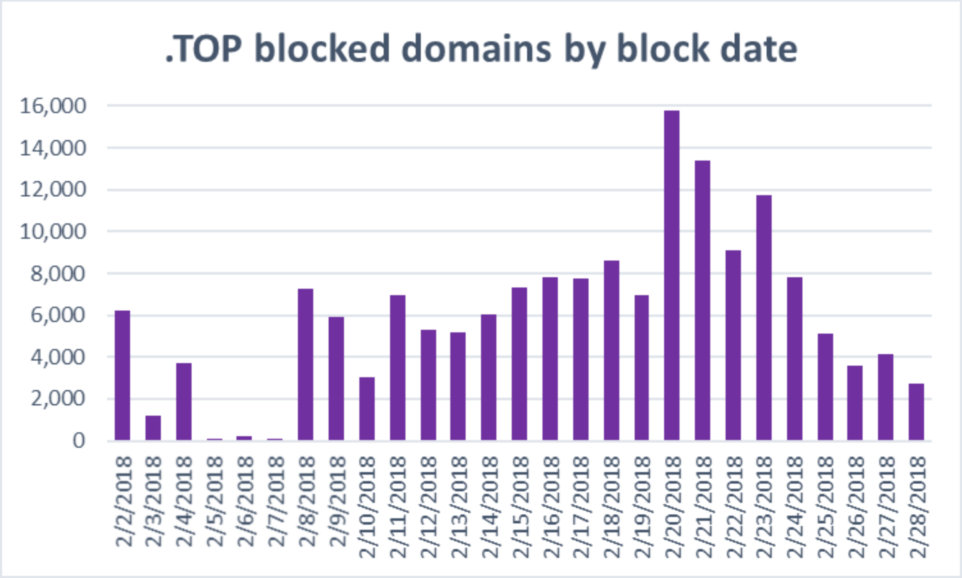


Chart 18: Blocklisting of .TOP domains in February 2018 study sample

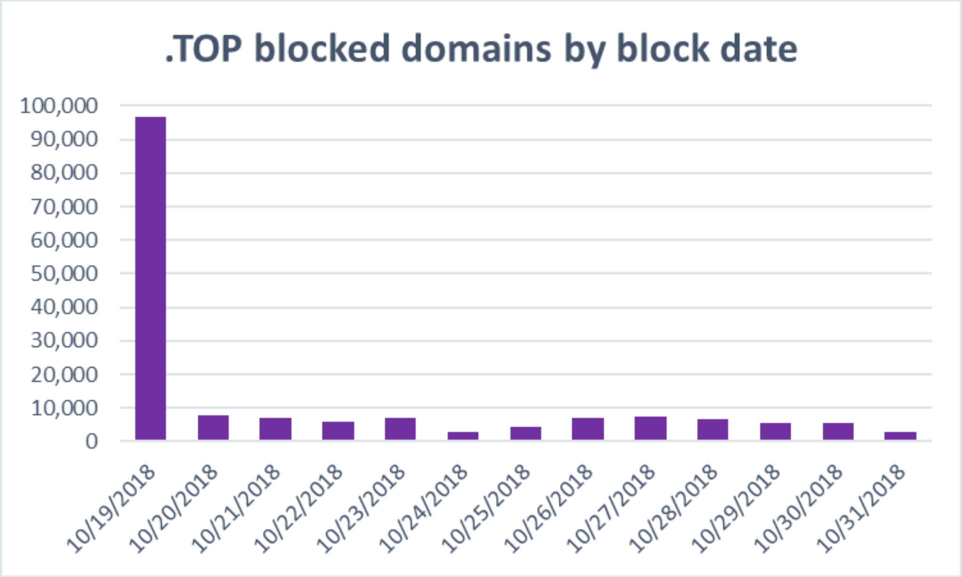


Chart 19: Blocklisting of .TOP domains in October 2018 study sample

In October 2018, we see a dramatic blocklisting event, again indicative of a snowshoe spam campaign. Without samples of emails or URLs of hosted content, we can only speculate that multiple unrelated campaigns ran simultaneously, or that conspirators coordinated a massive campaign.

Creation Date

In both samples, we find multiple dates where a significant or extraordinary number of domain names registered on a single date or range of dates were blocklisted. During our February 2018 study time period, over 7,000 domains were blocklisted that were registered on 1/24/2018, over 19,000 domains were blocklisted that were registered on 1/31/2018, and over 7,000 domains were blocklisted that were registered on 2/4/2018. We examined the 1/31/2018 creation date further when we studied registrants with high concentrations of blocklisted domains. The following chart depicts the count of blocked domains by registration date for the 84% of blocked domains in this sample that were registered after 10/1/2017.

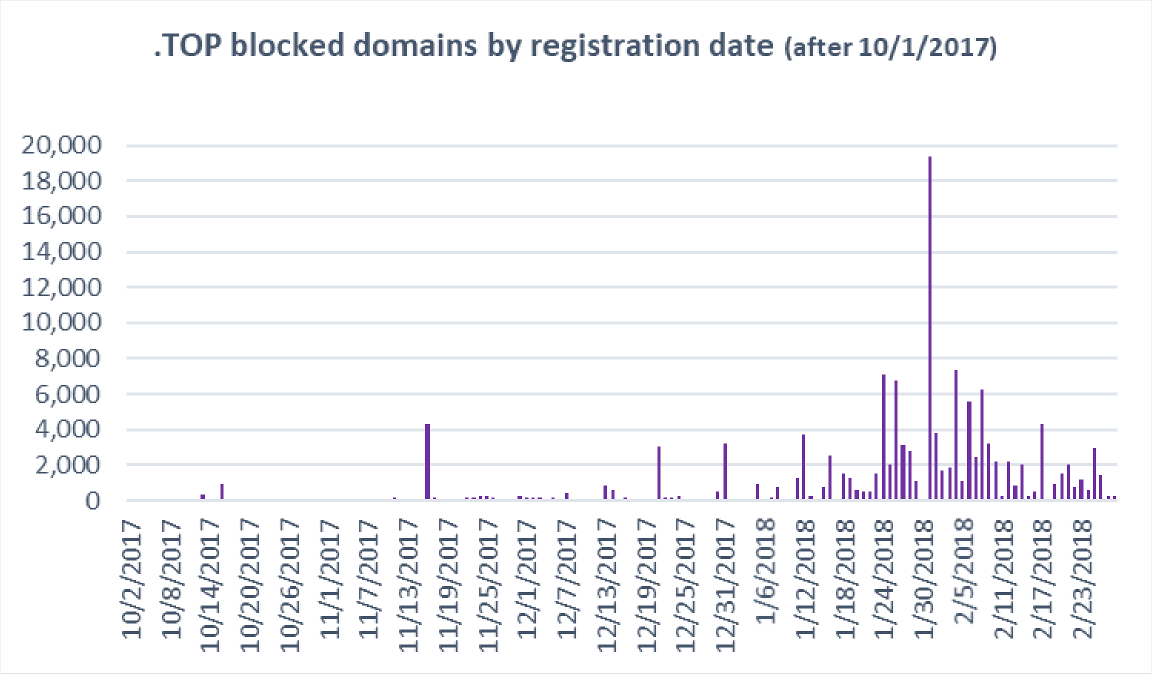


Chart 20: Registration dates of blocklisted .TOP domains in the February 2018 sample

During our October 2018 study time period, over 6,000 domains were blocklisted that were registered on 10/19/2018, nearly 6,000 domains were blocklisted that were registered on 10/24/2018, and over 8,000 domains were blocklisted that were registered on 10/25/2018.

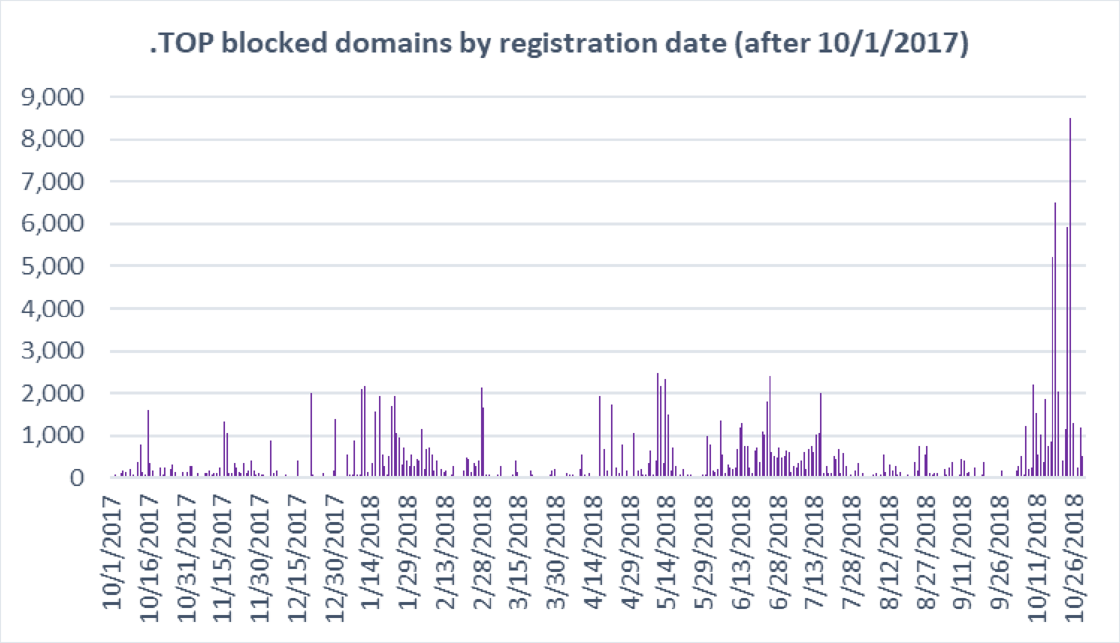


Chart 21: Registration dates of blocklisted .TOP domains in the October 2018 sample

Composition of 2nd level labels

As we observed in our other TLD samples, 2nd level labels of 6 or 7 characters are popular.

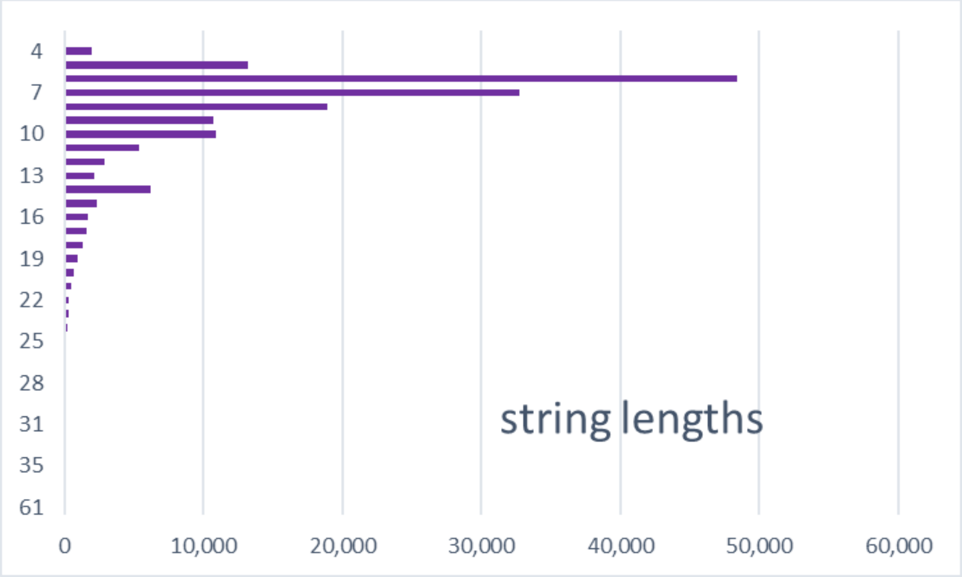


Chart 22: Distribution of 2nd level label lengths in February 2018 sample

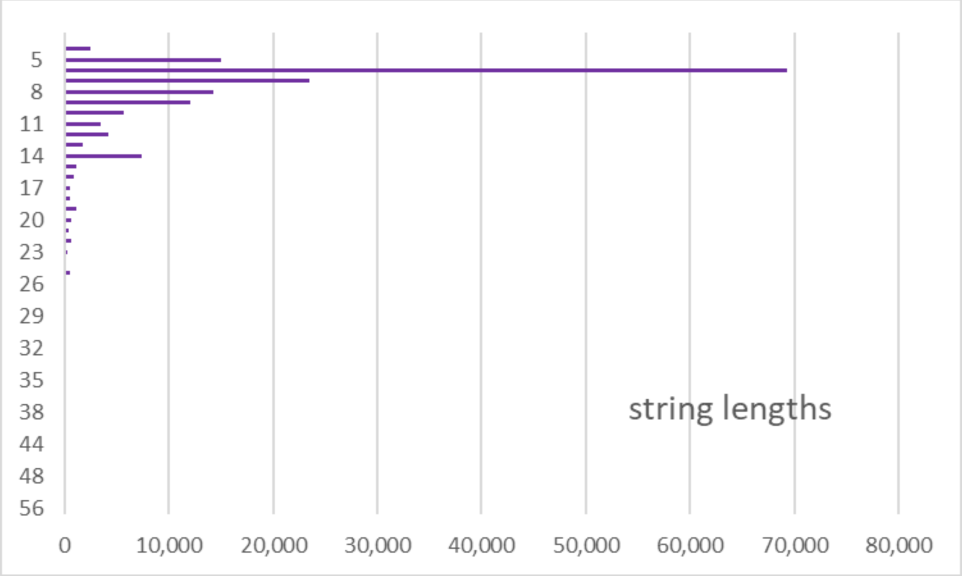


Chart 23: Distribution of 2nd level label lengths in October 2018 sample

Registrants with high concentrations of blocklisted domains in .TOP

We found several registrants with high concentrations of .TOP blocklisted domains in our February 2018 sample.

Registrant Name	Domains	Percent	Registrant Organization	Registrant Email
c◆e◆y◆b◆n	16,087	9.9	c◆e◆y◆b◆n	yubuko3281470@163.com
l◆u◆e◆g	8,976	5.5	l◆u◆e◆g	uak226620@163.com, 2736156318@qq.com
l◆ h◆n◆ y◆	8,377	5.1	l◆ h◆n◆ y◆	huaimiwang@163.com
j◆n s◆u◆i◆h◆a◆	6,509	4.0	j◆n s◆u◆i◆h◆a◆	wanjerng7@163.com
Whois Privacy Protection Service by onamae.com	5,859	3.6	Whois Privacy Protection Service by onamae.com	proxy@whoisprotectservice .com

Table 10: Registrants with high concentrations of .TOP blocklisted domains February 2018

The triplet {c◆e◆y◆b◆n, c◆e◆y◆b◆n, yubuko3281470@163.com} has an extraordinarily large number of blocklisted registrations in this .TOP sample. In .TOP, 15,602 domain names of length 6 characters (no hyphen) were registered on 1/31/2018 and 485 of length 7 characters (no hyphen) were registered on 2/21/2018. Registrations can only be processed at this volume through a bulk registration tool.

Threat Intelligence obtained through search-and-pivot

We found 19,268 domains registered by this contact data triplet in .TOP but did not find registrations in other TLDs. The registrant country in these registrations is CN. The registrant admin name, Nexperian Holding Limited, is associated with fraudulent online stores and multiple WIPO disputes (SUUNTO OY v. duan xiaosong, duan xiao song / Nexperian Holding Limited, WIPO Case No. D2017-0670; Van Cleef & Arpels, S.A. v. Neperian Holding Limited, WIPO Case No. D2017-0441; NXP B.V. v. Shen Zhen Shi Nan Huang Dian Zi You Xian Gong Si / Shenzhen nanhuang electronics co.ltd / Nexperian Holding Limited, WIPO Case No. D2017-0296; Visiomed Group v. Nexperian Holding Limited / Chu Huan Liu, Liu Chu Huan, WIPO Case No. D2017-0392.)

Registrant Name c◆e◆y◆b◆n has a concentration of domains hosted on addresses in prefixes allocated to ASN 26658 HENGTONG-IDC-LLC-HT (e.g., hrknfd.top,104.232.64.0/20) and to ASN 35908 VPLSNET - Krypt Technologies, US (e.g., aqexmm.top, in 67.229.32.0/22). Stopbadware identifies blacklist activity for 1104 IP addresses and 6639 malicious URLs in ASN 26658 and 1348 IP addresses and 2938 malicious URLs in ASN 35908.

The triplet {l◆u◆e◆g, l◆u◆e◆g, email uak226620@163.com} appears in over thirty-two thousand registrations. L◆u◆e◆g registered over 1000 domains on four dates in January 2018: 1,122 on 1/19/2018, 3046 on 1/24/2018, 2,716 on 1/26/2018, and 1,180 on 1/27/2018. These were classified as spam, phishing, or malware. The registrant country in these registrations is CN. The Administrative Name in thousands of these registrations where we found this triplet is again Nexperian Holding Limited.

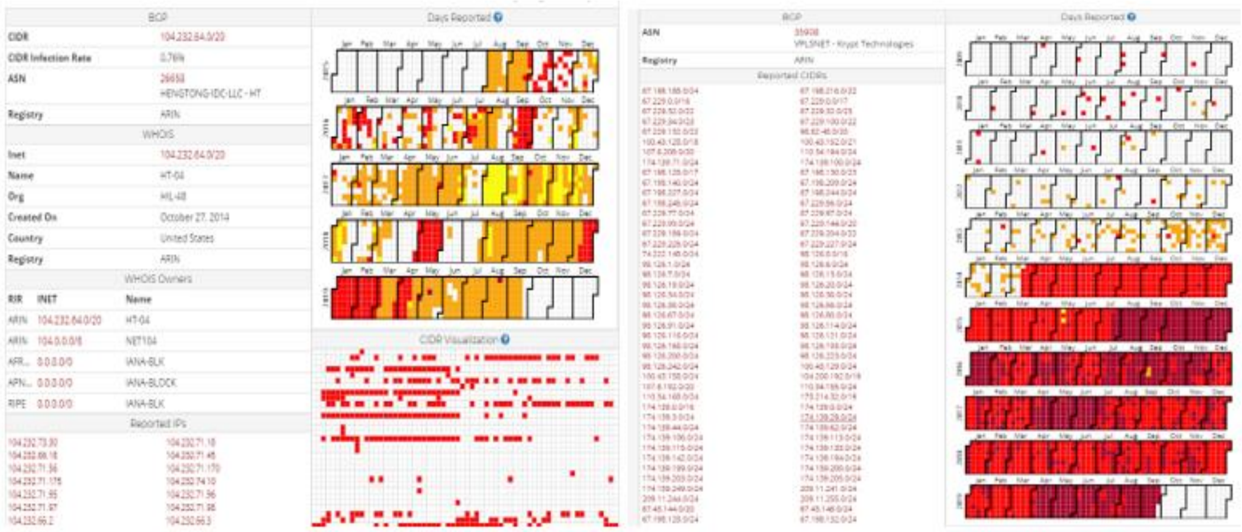


Figure 13: Heat maps of ASN 26658 and ASN 35908

We found a screenshot associated with multiple .TOP domains that is associated with a long-running fake dating scam. These domains were blocklisted for spam or phishing.

警告:未滿18岁者請勿進入japanese virgins！本站japanese virgins片源丰富,内容全面！注意自我保护，适度观看电影，合理安排时间，享受健康生活！

Warning: Those who are not 18 years yet please do not enter the site of Japanese Virgins. Our site has lots of videos, of all kinds! Please protect yourself, view the movies with caution, arrange your time well, and enjoy a healthy life.

Figure 14: Alleged phishing page linked to multiple blocklisted .TOP domains registered to chenyaban

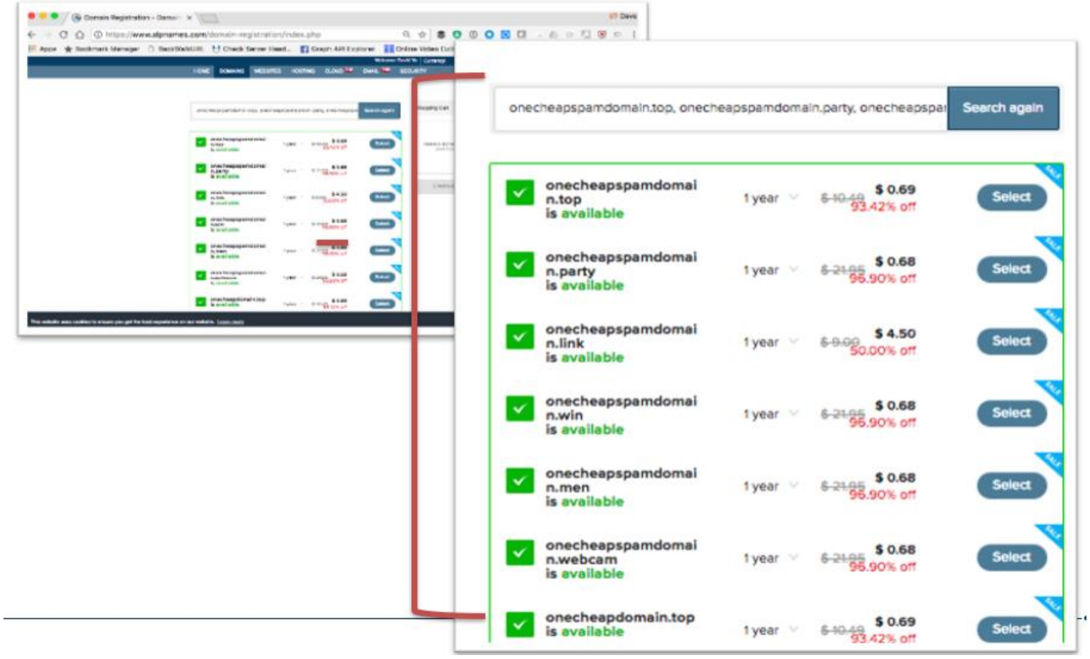
Redacted Whois records

We found several registrants with high concentrations of .TOP blocklisted domains in our October 2018 study; however, twenty-two percent of the domain registration records in our October 2018 sample were redacted for privacy.

Row Labels	Domains	Percent	Registrant Organization	Registrant Email
(blank)	36,571	22.0		
brave	13,627	8.2	brave	d◆p◆n◆e◆a◆s@yahoo.com
john	5,947	3.6	john	webmaster@healthynewsforyourday.com
L◆u Y◆n◆ B◆a◆	5,875	3.5	L◆u Y◆n◆ B◆a◆	35354413@qq.com
agle	5,778	3.5	agle	code9x9@hotmail.com
C◆e◆ D◆ G◆i	4,357	2.6	C◆e◆ D◆ G◆i	238476547@qq.com

Table 11: Registrants with high concentrations of .TOP blocklisted domains October 2018

The registration records of Registrant Names brave, john, and agle appear to be fraudulently composed and incomplete. AlpNames, Limited, is the registrar for these three registrants. AlpNames was notorious for "penny domain" registrations concentrated in the Famous Four Media portfolio of new TLDs. A March 2018 screen capture of AlpNames Limited's registration promotions appears in Figure 15.



onecheapspamdomain.top, onecheapspamdomain.party, onecheapspai

onecheapspamdomain.top is available — 1 year — ~~$ 10.49~~ $ 0.69 93.42% off — Select

onecheapspamdomain.party is available — 1 year — ~~$ 21.95~~ $ 0.68 96.90% off — Select

onecheapspamdomain.link is available — 1 year — ~~$ 9.00~~ $ 4.50 50.00% off — Select

onecheapspamdomain.win is available — 1 year — ~~$ 21.95~~ $ 0.68 96.90% off — Select

onecheapspamdomain.men is available — 1 year — ~~$ 21.95~~ $ 0.68 96.90% off — Select

onecheapspamdomain.webcam is available — 1 year — ~~$ 21.95~~ $ 0.68 96.90% off — Select

onecheapdomain.top is available — 1 year — ~~$ 10.49~~ $ 0.69 93.42% off — Select

Figure 15: A March 2018 screen capture of AlpNames, Limited's registration promotions

AlpNames provided a bulk registration service that allowed registrants to compose random-looking domains or domains containing one or more English language words. The three likely fraudulent registrants appear to have used this service:

- Registrant Name agle created five character random numeric 2nd level labels (07477.top, 92068.top) on 10/19.2018. These were blocklisted between October 20-2, 20186 and October 30, 2018.
- Registrant Name john created random-looking, 14 character 2nd level labels (0u1oa89inrq3hm.top, 1t50tz2pkbzsow.top) on January 11, 12, 18, and 23, 2018. These were blocklisted on 10/19/2018 for multiple strains of malware.
- Registrant Name brave created random-looking, 6 character 2nd level labels (afdwmz.top, juejoz.top) on 10/25/2018. These were blocklisted on 10/31/2018.

We chose to study the triplet {brave, lengdage, d•p•n•e•a•s@yahoo.com}.

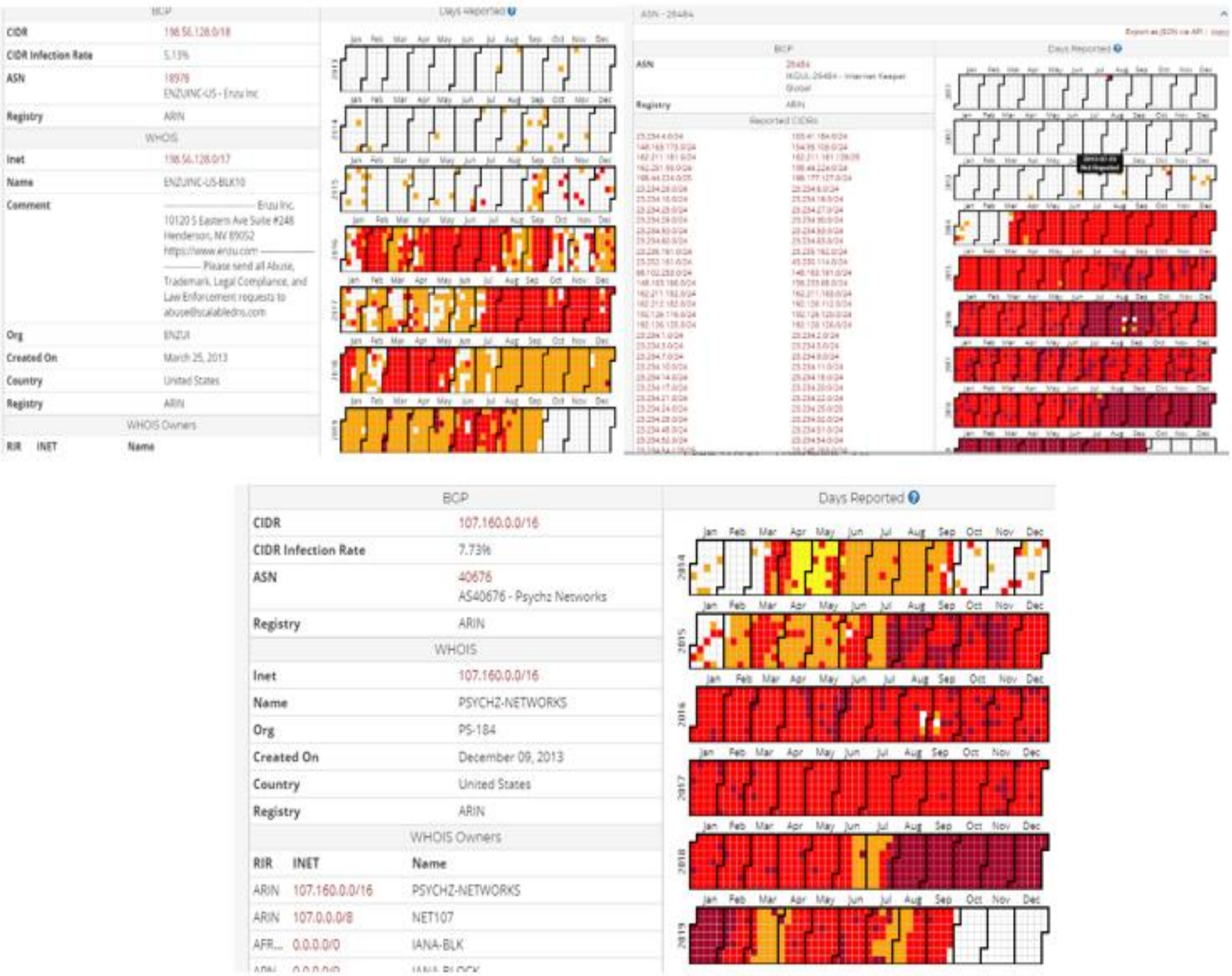
Threat Intelligence obtained through search-and-pivot

南通市通州区人民政府

We found a web page screenshot associated with a number of Registrant Name brave's domains, (e.g., adayfp.top, afiqsw.top, bikxbx.top, esiarg.top). This appears to impersonate the Chinese government site tongzhou.gov.cn. The domains are blocklisted for the presence of malware.

These fake pages were hosted at 198.56.177.21 from IP prefix 198.56.128.0/18 announced in ASN 18978 (ENZUINC-US - Enzu Inc), 156.235.19.106 IP prefix 156.235.19.0/24 announced in ASN 26484 (IKGUL-26484 - Internet Keeper Global), and 107.160.205.231 from IP prefix 107.160.0.0/16 announced in ASN 40676 (Psychz Networks).

These ASNs all have high infestations of malicious activity.



BGP	
CIDR	198.56.128.0/18
CIDR Infection Rate	5.13%
ASN	18978 ENZUINC-US - Enzu Inc
Registry	ARIN
WHOIS	
Inet	198.56.128.0/17
Name	ENZUINC-US-BLK10
Comment	———— Enzu Inc. 10120 S Eastern Ave Suite #248 Henderson, NV 89052 https://www.enzu.com ———— ———— Please send all Abuse, Trademark, Legal Compliance, and Law Enforcement requests to abuse@scalabledns.com
Org	ENZUI
Created On	March 25, 2013
Country	United States
Registry	ARIN
WHOIS Owners	
RIR INET	Name

ASN - 26484

Export as JSON via API

BGP	
ASN	26484 IKGUL-26484 - Internet Keeper Global
Registry	ARIN
Reported CIDRs	
[illegible]	[illegible]

BGP		
CIDR	107.160.0.0/16	
CIDR Infection Rate	7.73%	
ASN	40676 AS40676 - Psychz Networks	
Registry	ARIN	
WHOIS		
Inet	107.160.0.0/16	
Name	PSYCHZ-NETWORKS	
Org	PS-184	
Created On	December 09, 2013	
Country	United States	
Registry	ARIN	
WHOIS Owners		
RIR	INET	Name
ARIN	107.160.0.0/16	PSYCHZ-NETWORKS
ARIN	107.0.0.0/8	NET107
AFR...	0.0.0.0/0	IANA-BLK
ARIN	0.0.0.0/0	IANA-BLOCK

Figure 16: Heat maps of ASN 18978 (upper left), ASN 26484 (upper right), ASN 40676 (bottom)

We also found a web page screenshot of a Chinese lottery impersonation page at multiple domains (e.g., aivslr.top, dfkfjg.top auwvjn.top,). We determined that the legitimate web site is Www.950950.com. The logo at the impersonation page does not match the legitimate site. The domain is blocklisted as a phishing page. These and other of brave's domains were hosted at addresses announced in Psychz Networks, US, and PEGTECHINC - PEG TECH INC.

Domain name misuse in .US

Our primary source for composite blocklisting data provided gTLD samples. To study domain abuse in the ccTLD .US, we obtained blocklisted domain names directly from the Spamhaus Domain Block List (DBL) for a 14-day period that concluded on December 13, 2018. Our sample set contained 19,555 unique listed domains. At the writing of this report, the Spamhaus badness index for .US was 17.0%. .US currently appears on SURBL's Most Abused TLDs list. From Wayback Machine archives, we determined that .US has appeared regularly on the list in 2013, 2014, 2015, 2016, 2017, and 2018. .US is not among the most highly abused ccTLDs when the Spamhaus badness index is used for comparative purposes, but it is not among the least. SURBL counts the number of unique blocklisted domains daily, which indicates .US has a persistently daily high volume of criminal or attack domains.

Registrars with high blocklist concentrations in .US

One ICANN accredited registrar, NameCheap, Inc., accounts for more than 95% (18,587 of the 19,555) of the blocklisted domain names in our .US blocklist sample.

Registrar	Domains	Percent
NameCheap, Inc.	18,587	95.0
DNC Holdings, Inc.	410	2.1
(blank)	152	0.8
Dynadot LLC	130	0.7
GoDaddy.com, Inc.	89	0.5

Table 12: Registrars with highest concentrations of blocklisted .US domains in our sample

Insights from creation date

Chart 24 illustrates the creation (registration) date of the blocklisted names in our sample data. A large concentration of domain names that were blocked during our sample period were created on December 3rd and 4th, 2018, within our sample 14-day window. Previously, we demonstrated that criminals or attackers stockpile domains for a campaign or attack; here, we see that this is not always the case: some criminals or attackers register and immediately weaponize their domain names.

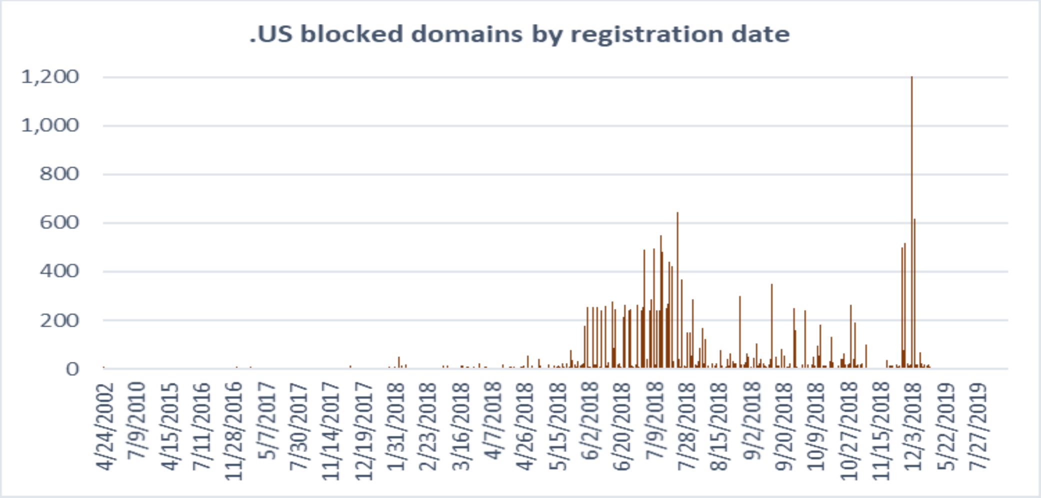


Chart 24: Registration dates of blocklisted .US domains

Composition of 2nd level labels

In this sample, the majority of blocklisted domains were four, five, ten, or eleven characters long. The four and five character 2nd level labels all begin with one or more numbers: single email domain alphamarketinggroup.biz is associated with 4,789 of these (two email accounts and two registrant names). This registrant merits deeper analysis as a bulk registration abuser.

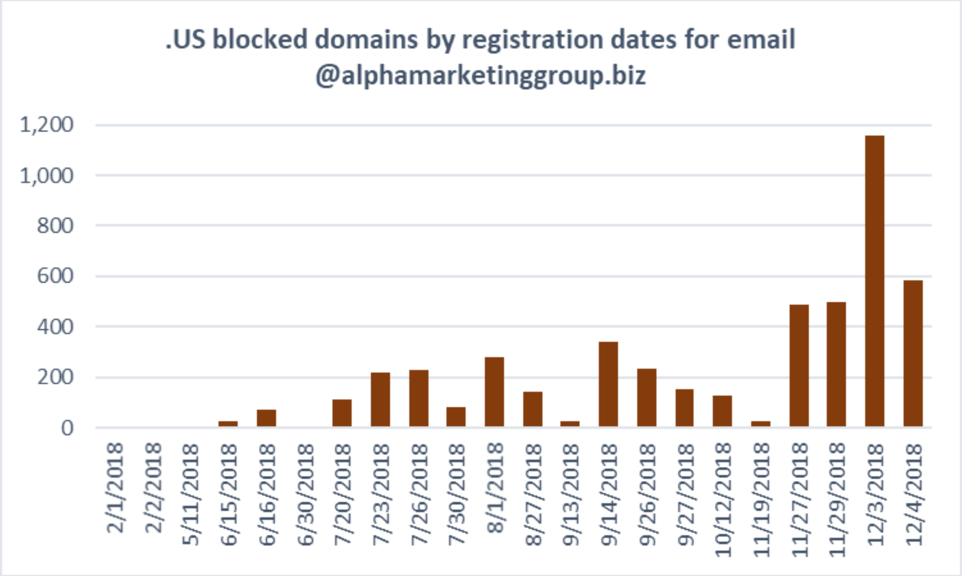
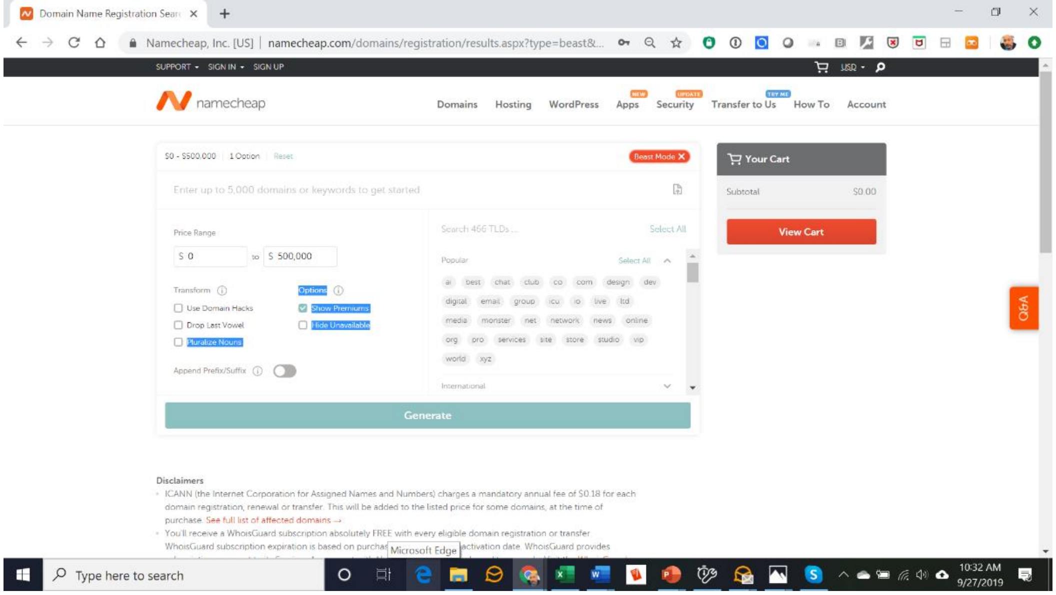


Chart 25: Registration behavior of alphamarketinggroup in December 2018 .US sample

Namecheap, Inc. offers a bulk registration service, Beast Mode. A registrant can choose TLDs, set a price range, select composition rules, and generate up to 5000 domains through a web form.



$0 - $500,000 | 1 Option | Reset

Enter up to 5,000 domains or keywords to get started

Price Range

$ 0 to $ 500,000

Transform

☐ Use Domain Hacks
☐ Drop Last Vowel
☐ Pluralize Nouns

Options

☑ Show Premiums
☐ Hide Unavailable

Append Prefix/Suffix

Search 466 TLDs ... Select All

Popular Select All

ai best chat club co com design dev digital email group icu io live ltd media monster net network news online org pro services site store studio vip world xyz

International

Subtotal $0.00

Disclaimers

- ICANN (the Internet Corporation for Assigned Names and Numbers) charges a mandatory annual fee of $0.18 for each domain registration, renewal or transfer. This will be added to the listed price for some domains, at the time of purchase. See full list of affected domains →
- You'll receive a WhoisGuard subscription absolutely FREE with every eligible domain registration or transfer. WhoisGuard subscription expiration is based on purchas activation date. WhoisGuard provides

Figure 17: NameCheap, Inc. Beast Mode bulk registration service

Registrants responsible for high concentrations of blocklisted domains

Of the 19,555 domain names in our sample, all but one had data in the Registrant email field. The Registrant Organization field of 17,450 domain names, however, was blank. One registrant has a high concentration of blocklisted US domains in our sample.

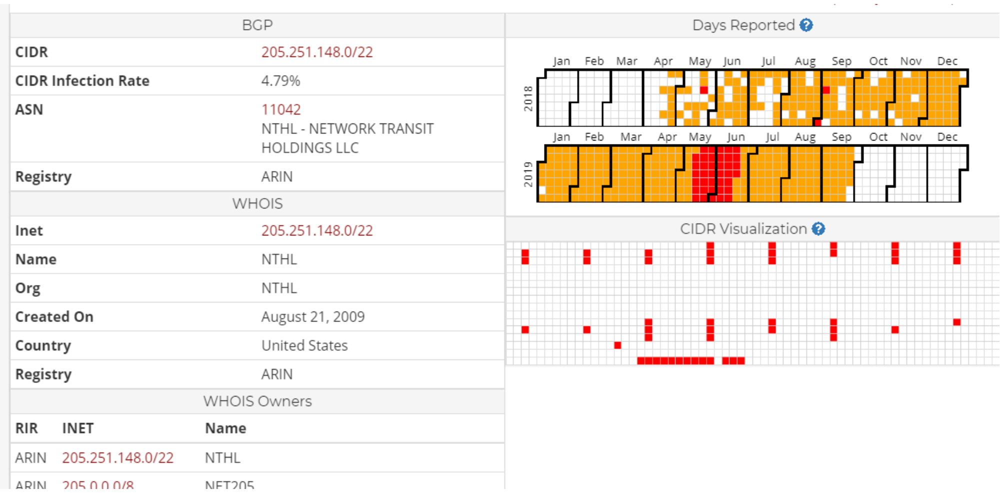
Registrant	Domains	Percent
R◆c◆ S◆a◆	4,029	20.6
A◆d◆e◆ S◆a◆	646	3.3
Q◆ Q◆n◆ J◆n	554	2.8
Domain Admin	533	2.7
A◆a◆ H◆r◆s◆i◆e◆	409	2.1

Table 13: Registrants with high concentration of blocklisted .US domains in our sample

Beyond the Top 5 in Table 13 we found a long tail: 12,265 of the remaining blocklisted domains in our sample are registered to fifty registrants, all having over 100 registrations, with an average of 245 registrations.

Threat Intelligence obtained through search-and-pivot

We searched the Domain Tools IRIS data with Registrant Name {A◆d◆e◆ S◆a◆ _or_ R◆c◆ S◆a◆} AND Registrant emails {a◆d◆e◆@alphamarketinggroup.biz, support@alphamarketinggroup.biz} and found 10, 682 historical Whois records in .US and 124 in .COM. The registrants indicated that they were US residents in the Registrant Country field. We narrowed our search to December 3, 2018 (1342 records) and December 4, 2018 (624 records) to find hosting intelligence related to our sample. We found a high concentration of mail server records at 205.251.151.106, an indication that the primary purpose of these domains was to emit spam. The address is allocated from IP prefix 205.251.148.0/22, announced in ASN 11042 NTHL - NETWORK TRANSIT HOLDINGS LLC. Stopbadware identifies blacklist activity at 149 IP addresses and 289 URLs in ASN 11042. Alpha Marketing Group (alphamarketinggroup.biz) appears to run affiliate program scams, e.g., they offer assistance with creating an online "Amazon Affiliate" business. They have no connection to the actual (and free) Amazon Associates program but take fees and fail to provide promised services. They have an "F" rating at the U.S. Better Business Bureau.



BGP

CIDR	205.251.148.0/22
CIDR Infection Rate	4.79%
ASN	11042 NTHL - NETWORK TRANSIT HOLDINGS LLC
Registry	ARIN

WHOIS

Inet	205.251.148.0/22
Name	NTHL
Org	NTHL
Created On	August 21, 2009
Country	United States
Registry	ARIN

WHOIS Owners

RIR	INET	Name
ARIN	205.251.148.0/22	NTHL
ARIN	205.0.0.0/8	NET205

Figure 18: Heat map of 205.251.148.0/22, in ASN 11042 NTHL - NETWORK TRANSIT HOLDINGS LLC

In summary, while we began with only partial Whois data, the presence of Registrant Name and Registrant email was sufficient to access complete historical Whois records collected elsewhere. With the complete records, we were able to determine that:

1. Two Registrant Names, associated with a single email domain, used NameCheap, Inc., to register domain names for scam spam campaigns.
2. The suspects composed random-looking domains when they registered in volume. The pattern of 2nd level label composition is one that NameCheap, Inc.'s bulk registration service, Beast Mode, supports.
3. The suspects concentrated registrations in .US but also registered some domains in .COM.
4. The domain names were identified as security threat (spam) and blocklisted by one or more reputation block list operators.
5. The suspects are associated with affiliate program scams.
6. The suspects took advantage of IP address space and ASNs that have a history of hosting security threats.

These findings should not be dismissed as a "content" issue. Advance or other fee frauds are not nuisance misuses of domain names. They are recognized as cybercrimes by the Council of Europe's Convention on Cybercrime. ICANN's Bylaws include the commitment to operate "for the benefit of the Internet community as a whole". Acting to protect the Internet community from misuse of domain names to point to or lure a user into a fraudulent transaction clearly falls within ICANN's remit.

Findings

For our first objective, we studied samples of security events where many thousands of domains were blocklisted in a relatively short time frame. From our studies of registrars that offer bulk registrations *and* also exhibit high concentrations of blocklisted domains for the Top-level Domains, and from our studies of the behaviors of domain registrants of the bulk registrations, we make the following findings.

1) Criminals take advantage of bulk registration services to “weaponize” large numbers of domains for their attacks. The date and time patterns of several blocklisting events that we studied are indicative of snowshoe spam campaign objectives: thwart detection by emitting spam from mail exchanges that are hosted at many IPs or at hostnames delegated from a large number of domain names, all registered to a common registrant.

2) Criminals who use bulk registration services share several observable behaviors:

   a) They register domain names in extraordinarily large quantities. Few legitimate purposes exist for accumulating thousands of domains over a short period of time. There may be organizations or individuals that register large numbers of domains for brand, intellectual property, or copyright protection, or for secondary marketing or domain speculation, but to our knowledge none of these have thousands of their registrations blocklisted or suspended following an attack or spam campaign, and none to our knowledge repeats this behavior.

   b) They repeatedly register very large numbers of domain names, in some cases over several months, before they launch attacks or campaigns.

   c) They often use random-looking 2nd level labels. Such labels have no apparent legitimate uses: they don’t represent businesses, products, services, novelties, or ideas. Random-looking names do appear to have a value to criminals: it is unlikely that they would “collide” with legitimate registrant names and criminals thus avoid efforts that organizations employ to protect against registrations of strings in which they have an intellectual property or copyright interest.

   d) Certain criminal registrants appear to have “registrar loyalty”. We found evidence that that they registered domain names through the same registrar for many years.

   e) Certain criminal registrants use automation provided by registrars to register domain names at a rate that humans cannot achieve by individual name submission, e.g., dozens or hundreds of domains in minutes.

   f) Criminal registrants may concentrate registrations in one TLD, but they are either agnostic about the TLD or a factor such as pricing influences which TLD they exploit.

3) Our suspects appear to concentrate their registration activity at registrars AlpNames Limited, Alibaba Cloud Computing Ltd. d/b/a HiChina, Chengdu West Dimension Digital Technology Co., Ltd., GMO Internet, Inc., and Namecheap, Inc. These registrars have appeared on the Spamhaus Most Abused Registrars list on one or more occasions; for example,

a) AlpNames was #1 on July 13, 2017, #1 on October 18, 2018, and #3 on January 13, 2019;
b) Namecheap appeared as #7 on February 9, 2017;
c) GMO Internet, Inc., was #2 on July 13, 2017, #5 on October 18, 2018, and #3 the time of writing of this report; and
d) Chengdu West Dimension Digital Technology Co., Ltd. was #6 on January 13, 2019.

GMO Internet, Inc., Alibaba Cloud Computing Ltd. d/b/a HiChina, and Namecheap were also reported as having high concentrations of malicious domains in Domain Tools' 2016 report Distribution of Malicious Domains. These registrars all offer bulk registration services and registration pricing that attracts criminals or attackers, who are no different from any business operator and constantly seek low cost of execution.

These findings are not novel to this study. They reinforce the Internet security industry's widely held perception that these registrars are a locus or haven for spammers. They also corroborate findings from a report, Statistical Analysis of DNS Abuse in gTLDs (SADAG), commissioned and published by ICANN organization in 2017.

For our second objective, we demonstrated how investigators use Whois records to associate portfolios or sets of domains with perpetrators of cyberattacks or cybercrimes. We have illustrated how investigators can begin with a single domain in a targeted TLD and, by using Whois, expand the investigation to other TLDs where the actors have registered domains for the crime. We show how complete Whois records can lead investigators to identify the criminal act in-progress or even after the attack has concluded. We show how evidence of an attack can be collected from captured screenshots, search engines, IP abuse data, malware analysis data, and information sharing among private sector investigators, law enforcement, and researchers.

We make the following findings.

1) Privacy protection services or redaction of Whois point of contact information to comply with the EU General Data Protection Regulation (GDPR) or ICANN's Temp Spec introduce an additional level of complexity for investigators. When complete Whois records are not available, less usable information is available, in real time and historically, and investigators cannot make all the necessary correlations to map a criminal domain infrastructure or to assist in attributing the criminal activity to a perpetrator(s). Suppression of contact data also strips investigators of names or email user identities ("handles") that could be used to search for criminal actors in social media or other online forums

2) Criminals are unlikely to provide accurate data. Criminals or attackers aggressively register domains using fraudulently composed or incomplete Whois information. Using bulk registration services, they can register hundreds or thousands of domains for abusive or criminal purposes without accountability.

3) The "search and pivot" value of data contained in complete Whois records is essential for timely intervention or research. When complete Whois records are available, investigators are able to *quickly* attribute criminal or abuse activities for purposes of triage (suspension of name resolution, domain seizure) and thus mitigate harm or loss. When investigators can access complete historical Whois records, researchers can conduct longitudinal studies (the ICANN DAAR project is one such

activity) or focused studies such as this report or the aforementioned SADAG report commissioned by ICANN.

4) Timely and uniform access to Whois contact data expedites cybercrime detection, intervention, and triage. Redacting Whois contact data, offering privacy protection for free, and rate limiting Whois queries impede these efforts.

5) Although complete and accurate Whois data is most helpful in victim identification or notification, until registries or registrars are obliged to validate domain registration data, “poor data is better than no data”. We demonstrated that while alternative investigative techniques can make use of even fraudulent or incomplete data in Whois (e.g., using string patterns observed in 2nd level labels, or analyzing creation dates, registrar, or other Whois data fragments), these techniques are necessary but not sufficient to attribute criminal actions to criminal actors. Specifically, we demonstrated that investigators can gather inferences by pivoting from public Whois data to other threat intelligence data but without contact data, investigators cannot produce actionable results in as timely or complete a manner as near-real time access to complete Whois data, which very commonly provides investigators with a suspect in a few seconds.

Absent any change of policy at ICANN, we anticipate that response to and full investigation of cybercrimes or cyber attacks will continue to be encumbered by lack of information. Consequently, we expect attackers will benefit from longer windows of opportunity for their criminal or other threats to public safety.

Corroborating earlier studies

A March 2019 article, Facts & Figures: Whois Policy Changes Impair Blocklisting Defenses, reports an Interisle collaboration with block list services Spamhaus and SURBL to observe the effects that the redaction of Whois contact data has on blocklisting domains. That study showed a drop in the number of criminal or cyber domain names that are identifiable, and thus trackable using Whois contact data, after May 25, 2018. In this study, we were able to associate suspects with known spammers because we had complete Whois records for domains registered prior to May 25, 2018. We can corroborate findings from Spamhaus and SURBL that blocklist operators and researchers “*are unable to determine whether registrations created after May 25, 2018 are part of a known criminal actor’s arsenal of domains, which also adversely affects the ability to separate good from bad. Knowing who the good actors are is extremely valuable information in conducting threat assessment.*”

ICANN should not dismiss these findings as “content” issues. These acts are not nuisance misuses of domain names but security threats—malware, spam, phishing—that are recognized as cybercrimes by the Council of Europe’s Convention on Cybercrime. Cheap domain names contribute to a criminal marketplace where small investments can yield extraordinary returns. Consider the investment in a ransomware attack:

- Mailing lists can be purchased in the Dark Web or online, or created using email harvesters, again available from github.
- 1000s of domain names can be acquired for pennies per domain from registrars like GMO Internet, Inc.

- Malware can be purchased through Ransomware as a Service (RAAS) as cheaply as $39.00. Similar opportunities exist for acquiring Phishing kits (PhAAS), or they can be downloaded for free from programming repositories such as github. Online tutorials are available from YouTube for novices.

Assuming a ransomware extortion fee of $200-500 USD, a ransomware attack can be profitable with fewer than a dozen victims. Multiple, successful ransomware campaigns yielding thousands of victims is within reach, making this criminal activity a possible $1M/year enterprise.

Recommendations

Bulk registration services, as currently offered, create opportunities for cyber criminals to register and weaponize hundreds, thousands, or tens of thousands of domain names with unvalidated credentials at attractive pricing. Criminals accrue several advantages from these opportunities, including infrastructure diversity and resiliency, virtual anonymity, and low cost of operation. They are able to employ botnet, fast flux, snowshoe, or other evasion techniques that rely on large numbers of domain names and IP addresses to defeat or delay detection and mitigation efforts.

The post-GDPR environment in which domain name registration data is not readily available creates corresponding operational challenges for investigators. Detection and mitigation as well as the ability to quickly and effectively identify criminals are more complicated. Large-scale attacks create extraordinary risks to public safety, including but not limited to financial fraud, extortion, election interference, and political influence campaigns.

We recommend that the ICANN organization and community consider the following Consensus Policies which, if adopted *and incorporated into contracts*, would contribute to reducing cybercrime and mitigating its effects on victims. These policies could be proposed to the ICANN Security, Stability, and Resiliency Review Team (SSRRT), the Security and Stability Advisory Committee (SSAC), or the Governmental Advisory Committee (GAC). Those bodies in turn could recommend the initiation of an appropriate policy development process.

Recommendation 1. Validate domain name registration data.

Include verification of registrant payment methods as part of the validation process; for example, decline transactions in which the registrant contact data does not match the authorized credit card user. Do not permit anonymous or non-traceable payment methods. Validate all changes to registration data.

Validation of domain registration data should be the goal for **all** gTLD and ccTLD domain names; however, the scale and impact of bulk registration misuse demands immediate steps to validate bulk registrations.

Rationale: Other industries recognize and accept their obligation to protect the public from (criminal) misuse of potentially dangerous products through mandatory or recommended validation regimes. U.S. pharmacies, for example, require valid proof of identification from any party that attempts to purchase quantities of pseudoephedrine that exceed well-defined limits. Legitimate businesses comply with these and like-minded regulations in the interest of public safety.

The legitimate businesses that register hundreds or thousands of domain names should accept a similar responsibility. A validation policy would make it more difficult for to register domains for criminal purposes with minimal inconvenience to non-criminal enterprises. Some registrars validate account creation today; for example, Alibaba Cloud Computing sends a confirmation URL to the email address of the account creator or a verification code to the account creator’s mobile number.

Recommendation 2. Define “bulk registrant” as a new element of registration data for Whois.

The registration data for every domain name should include a flag that indicates whether or not the domain name was registered as part of a bulk registration.

Rationale. This study has demonstrated that criminals routinely and repeatedly weaponize domain names using bulk registrations. The “bulk registrant” data element could be used to track or ban an abusive registrant across delegated gTLDs. Other resources that can be weaponized are tracked in similar ways; for example, tracking regulations apply to sellers of ammonium nitrate in the USA. These exist to protect the public against the construction of improvised explosive devices. Most ammonium nitrate purchases are legitimate; so are most domain name registrations. But just as ammonium nitrate safety measures protect the public from acts of terrorism, this policy would protect the public from misuse of domain names for extortion, fraud, or other criminal acts.

Recommendation 3. Define an Acceptable Use Policy (AUP) that applies specifically to parties that register large numbers of domains.

The AUP should state that criminal abuse of a domain name is a violation of the service agreement between the registrant and the registrar; that the registrar will cooperate with the relevant registry to immediately suspend name resolution for an abused domain pending investigation of any complaint of AUP violation; and that the registrar may suspend access to the registrant’s account entirely after repeated AUP violation.

Rationale: Registrants that seek to register large numbers of domain names should provide a legitimate reason for doing so and should be held accountable for and subsequent abuse. Legitimate registrants, especially those who are familiar with intellectual property, copyrights, or domain name protection will see the value of such a policy.

Recommendation 4. Require registrants to apply for bulk registration services.

Registrars should offer bulk registration services only after validating an application from the prospective registrant. Regional Internet Registries (RIRs) have experience managing IP address allocations to prevent excessive consumption or misuse of IP prefixes. The requirements and assessments that RIRs use to determine whether or not to allocate an IP prefix is a useful model for bulk registration services.

Rationale: Because of its potential for weaponization, bulk registration should be subject to additional scrutiny to prevent abuse.

Recommendation 5. Distinguish domain names registered by legal entities from those registered by natural persons, classify parties that use bulk registration services as legal entities, and require unredacted access to the registration data of legal entities.

Rationale: Current privacy regulation, including the GDPR, observes a distinction between individuals and legal entities, and places no obligation on ICANN (or its accredited registries and registrars) to redact the registration information of legal entities in responses to Whois queries.

Recommendation 6. Maintain and publish a current list of validated bulk registrants.

Require registrars to share data on validated bulk registrants among themselves and with ICANN.

Rationale: Investigators can incorporate this information into their abuse or security threat detection methodologies to minimize false positives. Sharing this information also enables registrars to identify bulk registration behavior involving different or innovative registration patterns not yet observed in the wild.

Recommendation 7. Disallow registration transactions that involve large numbers of random-looking algorithmic domain names.

Require registrars to block these transactions and report them to ICANN. Techniques such as those described in Automating Detection of "Random-Looking" Algorithmic Domain Names can be used by registrars or registries to recognize this form of registration misuse.

Rationale: Random-looking algorithmic domain names are commonly employed for criminal activities.

Recommendation 8. Disallow, for a period of one year, the re-registration of any bulk-registered domain name that has been used in a criminal cyberattack.

These domain names should not resolve in the public DNS except where a court order or a collaborative sinkholing arrangement between the registrar and a third party exists.

Rationale: Once weaponized, a domain name has a persistence value. Resolution of a domain name may be suspended but an email that contains a weaponized domain name or URL may remain unread. Simlarly, suspension of name resolution does not ensure that malicious content is removed from a host. Criminals are known to re-register domain names that they have previously weaponized.

Recommendation 9. Provide the ICANN DAAR project with access to unredacted Whois data without rate limiting.

Secure this access with explicit registry and registrar contract terms.

Rationale: According to the DAAR methodology white paper, statistics including monthly and 365-day rolling cumulative counts (per registry and registrar) of domains that have been added to at least one of DAAR's reputation data feeds offer insights into bulk registration behavior. These measurements cannot be made accurately while information redaction and Whois rate limiting interfere with data collection.

Acknowledgements

We wish to acknowledge Domain Tools, Inc., Seclytics, Inc., The Spamhaus Project, and iThreat Cyber Group for their support of this study. We also thank Greg Aaron and Jeff Chan for their participation in research and contributions to this report.