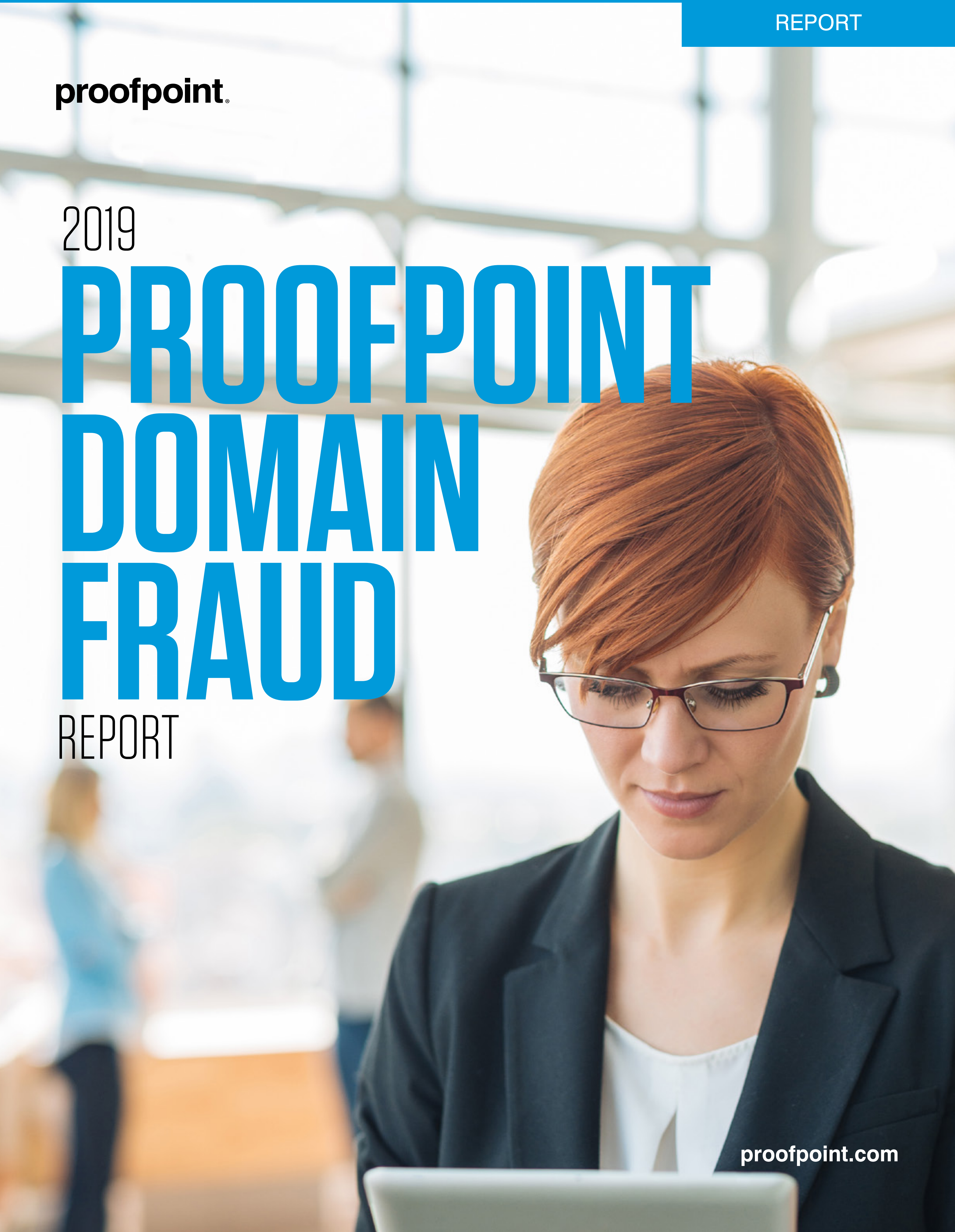
REPORT



2019 PROOFPOINT DOMAIN FRAUD REPORT

proofpoint.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Domain fraud is an attractive attack method used by cyber criminals. Cheap and easy domain registrations create a low barrier to entry. Privacy features offered by most registrars and regulations like European Union General Data Protection Regulation (GDPR) have made it easy to remain anonymous. And, most important, fraudulent domains provide the basis for a wide range of attacks such as wire transfer fraud, phishing, counterfeit good sales, scams and other new attacks.

Like many of today's most pressing cyber threats, domain fraud targets people rather than infrastructure. Bad actors use social engineering to trick people into believing their domains are legitimate. And often, they are effective.

This Domain Fraud report outlines our latest research on domain trends, including the tactics and activity of the domains defrauding top global businesses and their customers. Here are our key findings.

As the domain universe grows, so do fraudulent domains. Quarterly domain registrations grew 44% between Q1 and Q4 2018. Registrations of fraudulent domains also increased 11% during the same period. Threat actors register millions of new fraudulent domains each year, targeting customers and employees of top enterprises. Fraudulent domains use many of the same top-level domains (or TLDs—common internet address suffixes such as ".com" and ".org")—as legitimate domains do. And fraudsters are registering these domains using many of the same registrars, too.

Most businesses are affected by fraudulent domains. Our research found that businesses across industries and geographies are at risk from fraudulent domains. 76% of Proofpoint Digital Risk Protection customers found "lookalike" domains posing as their brand. In retail, domains devoted to selling counterfeit goods are a compelling threat. More than 85% of top retail brands found domains selling knockoff versions of their products. In fact, the average retail brand had more than 200 such detections.

Fraudulent domains are active and positioned for an attack. Most fraudulent domains detected are active, with more than 90% associated with a live server. More than 15% have mail exchanger (MX) records, indicating that they send and/or receive email. And 1 in 4 have security certificates, which many internet users mistakenly equate with legitimacy and security.

Fraudulent domains are using email for highly targeted attacks. For 94% of Digital Risk Protection customers, we found at least one fraudulent domain posing as their brand and sending email. We also saw fraudulent domains sending low volumes of email, behavior typically associated with highly targeted and socially engineered attacks.

Market factors, such as the introduction of new TLDs, create opportunity for threat actors. In 2018, the introduction of new TLDs, such as .app and .icu, provided new opportunities for the registration of fraudulent domains. Our research suggests that attackers rushed to register domain names with the new TLDs. These fraudulent domains resembled ".com" domains already owned by top brands. Google's .app TLD, for example, was an especially attractive target.

METHODOLOGY

Proofpoint's Active Domains Database leverages multiple WHOIS data sources, Proofpoint email visibility and other proprietary Proofpoint data sources to create the most comprehensive and accurate record of global domains daily. Unless indicated, all data represents the period between January 1, 2018 and December 31, 2018. Additionally, the domain "created date" is not always available in WHOIS records, which means some domains, TLDs or registrars may not be accounted for in sections related to 2018 registrations. To identify registrars, Proofpoint researchers used IANA identification numbers, which are not always available in WHOIS responses.

DOMAIN TRENDS

Our research team uses a highly scalable detection system to continually analyze over 350 million domains—virtually all domains on the web—in the Proofpoint Active Domain Database. This analysis helps us identify domain trends on a global and regional scale.

REGISTRATIONS

The domain universe grew substantially in 2018. New registrations outpaced domain expirations, drops and deletes. On a month-to-month basis, growth ebbed and flowed. These changes reflect the dynamic nature of the domain market, continuously fluctuating prices, the launch of new TLDs and other factors.

New Registrations Outpace Expirations

189,032

Average number of domains registered each day in 2018

159,124

Average daily number of domains dropped, deleted or allowed to expire in 2018

IN 2018

Total Active Domains

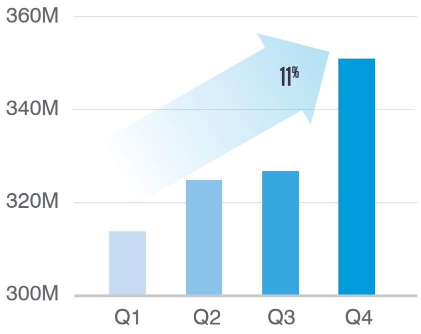


Figure 1. The total number of domains increased by 11% between Q1 and Q4.

Total Active IDNs

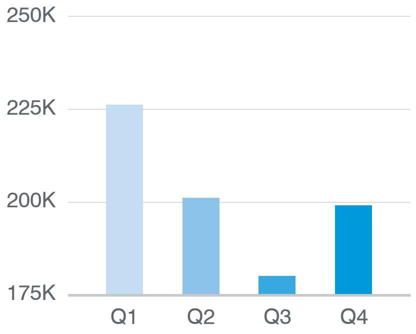


Figure 2. Internationalized domain names (IDN), which utilize non-ASCII characters, decreased between Q1 and Q3 before rising again in Q4.

Newly Registered Domains

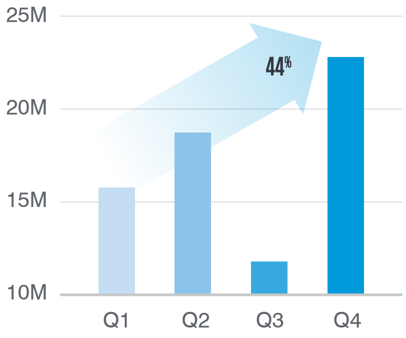


Figure 3. New domain registrations fluctuated from quarter to quarter, but increased by 44% between Q1 and Q4.

CHARACTERISTICS

Across all domains

66% resolve to an IP address, indicating that they are associated with a live server

53% have an HTTP response, indicating that the domain is hosting web content and responds to an HTTP request

42% have an MX record, meaning that the domains are configured to send and/or receive email

6% have a security certificate, meaning that communications between the browser and the web server are encrypted

There are more than 14 million unique IP addresses associated with the observed domains. Most of these IP addresses host just one domain or a handful of domains. But a small percentage (less than 2%) host significantly more. In fact, more than 40% of resolved domains (120 million) are hosted by just 406 unique IP addresses (Figure 4).

This lopsided concentration may have several causes. Speculative domain purchasers often leave such domains resolving to a common default “under construction” page provided by the registrar or web hosting provider, for instance. Businesses that manage many domains may also use a single IP address to conserve resources.

But a number of these shared IP addresses are also likely controlled by “parking groups.” These can represent a threat. (See the section “PARKED DOMAINS” on page 17 for more on this trend.)

Because so many domains use shared IP addresses (often for innocuous reasons), condemning or validating a domain based on IP address alone can be impossible. One fraudulent domain using an IP address does not necessarily mean that all other domains using that address are fraudulent. Determining the trustworthiness of a domain requires a broader analysis.

Domains with MX records use MX servers to send and/or receive email. Domain owners may host such servers themselves or use shared servers, frequently offered by hosting providers. A typical domain uses between one and five MX servers. Figure 5 and Table 1 show the breakdown of MX servers across domains with MX records. Note that No. 19 on the list of shared MX servers does not point to an actual server, indicating that the domain can not receive email. Domains using shared MX servers are more likely to use multiple servers than those using self-hosted MX servers.

Top Shared MX Servers Used by Domains

1. secureserver.net
2. google.com
3. registrar-servers.com
4. googlemail.com
5. outlook.com
6. kundenserver.de
7. ovh.net
8. b-io.co
9. 1and1.com
10. one.com
11. 123-reg.co.uk
12. rzone.de
13. 1and1.co.uk
14. ctmail.com
15. mailspamprotection.com
16. hostedemail.com
17. gandi.net
18. qq.com
19. localhost.
20. zoho.com

Table 1

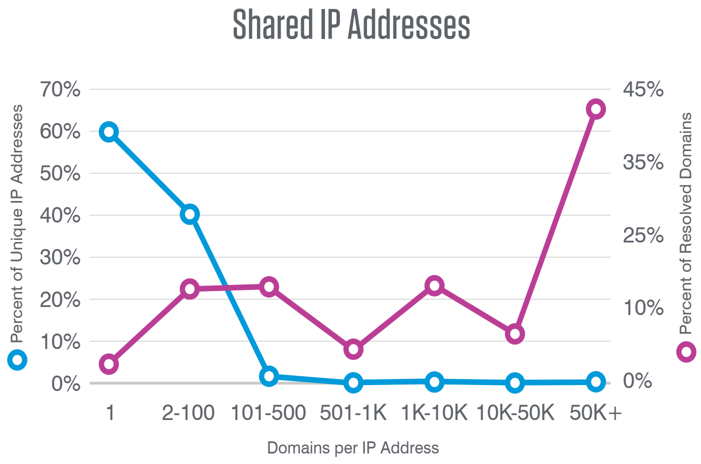


Figure 4

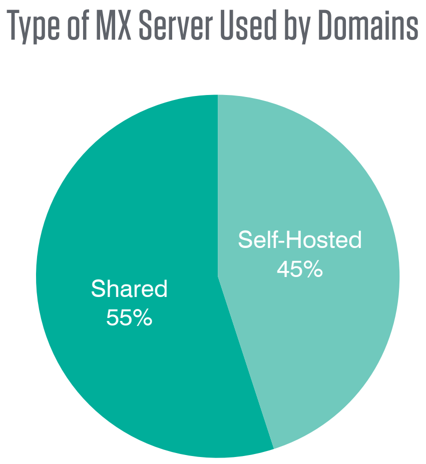


Figure 5

TOP-LEVEL DOMAIN TRENDS

There are now more than 1500 TLDs available for registration,[1] including more than 300 country-code TLDs (ccTLDs) and a growing list of more than 1200 generic TLDs (gTLDs).[2] Figure 6 and Figure 7 show the top TLDs for new domain registrations in 2018.[3]

On a monthly basis, ".com" held a consistent position as the most popular TLD for new registrations. The rest of the TLD landscape shows pronounced fluidity from month to month. Popularity also appears to be heavily influenced by factors such as pricing and availability. When new TLDs are launched, speculators and businesses often rush to register new domains with them.

As an example, note the surge of ".app" registrations in May. For other TLDs, registrations spike in response to discounts by registrars. This trend may explain the increase in ".ooo" registrations in June and August, when flash sales brought the cheapest available price for that TLD from $24 to $2. Conversely, registrations with ".loan" dropped significantly in August, when the cheapest registration price climbed from under $1 to more than $10. The ".biz" TLD experienced a huge spike in registrations in May, nearly all of them through Chinese internet giant Alibaba Group, perhaps prompted by a flash sale.[4]

For some TLDs, registration growth was especially rapid over the course of 2018 (Figure 8).

Top-Level Domains Registered by Month

RANK	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
1	com	com	com	com	com	com	com	com	com	com	com	com
2	top	top	loan	loan	biz	loan	top	top	top	net	net	net
3	net	loan	xyz	top	top	cn	cn	club	cn	top	xyz	site
4	org	net	net	net	cn	top	net	cn	net	xyz	top	top
5	cn	org	org	cn	org	net	org	net	org	site	ltd	online
6	club	ru	cn	org	app	org	co.uk	org	xyz	org	org	org
7	info	co.uk	ru	co.uk	net	club	loan	info	co.uk	info	site	xyz
8	xyz	info	top	ru	co.uk	ooo	info	co.uk	info	us	club	info
9	co.uk	cn	co.uk	info	ru	co.uk	xyz	ooo	work	co.uk	ru	icu
10	ru	xyz	info	xyz	info	info	ru	xyz	club	ru	info	ru

Figure 7

Top 10 TLDs by New Registrations

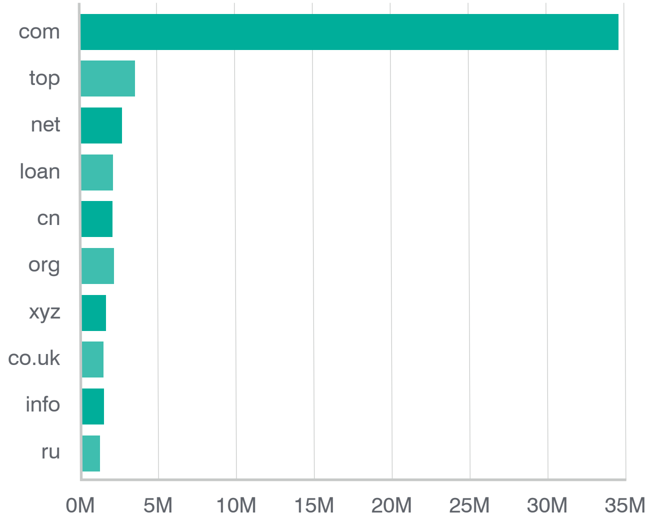


Figure 6

Top 10 Fastest Growing TLDs by New Registrations

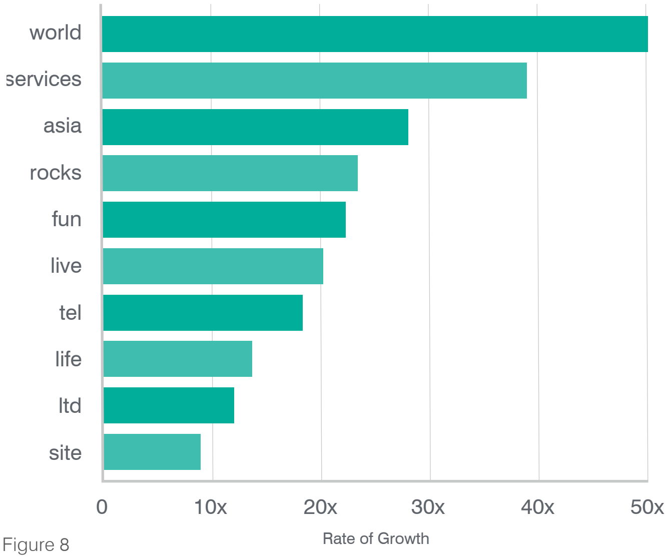


Figure 8

[1] ICAAN. "List of Top-Level Domains." Accessed April 2019.
[2] ICAAN. "Program Statistics: Current Statistics." Accessed April 2019.
[3] Some TLDs do not report the "created date" for their domains, so they may not be represented in this analysis.
[4] Historical price trends sourced from: https://tld-list.com

REGISTRARS

A domain-name registrar manages the registration of domain names and must be accredited by a generic top-level-domain (gTLD) registry or a country-code top-level-domain (ccTLD) registry. A business must be accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) before they can become a domain registrar for the ".com," ".net" and ".name" TLDs.

Top Registrars Across All Domain Registrations

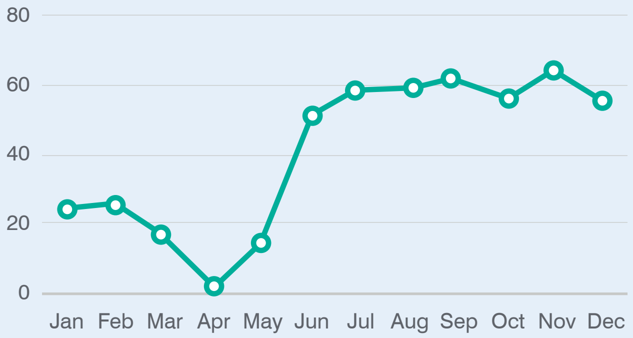
1.	GoDaddy.com, LLC.	24%
2.	NameCheap, Inc.	8%
3.	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	5%
4.	Alibaba Cloud Computing (Beijing) Co., Ltd.	5%
5.	Tucows Domains Inc.	4%
6.	GMO Internet, Inc. d/b/a Onamae.com	4%
7.	Chengdu West Dimension Digital Technology Co., Ltd.	3%
8.	Xin Net Technology Corporation	3%
9.	PDR Ltd. d/b/a PublicDomainRegistry.com	3%
10.	Network Solutions, LLC.	2%
11.	NameSilo, LLC.	2%
12.	Alibaba.com Singapore E-Commerce Private Limited	2%
13.	Google LLC	2%
14.	1&1 Internet SE	2%
15.	eNom, LLC	2%
16.	West263 International Limited	1%
17.	OVH sas.	1%
18.	Dynadot, LLC.	1%
19.	FastDomain Inc.	1%
20.	Name.com, Inc.	1%

Table 2

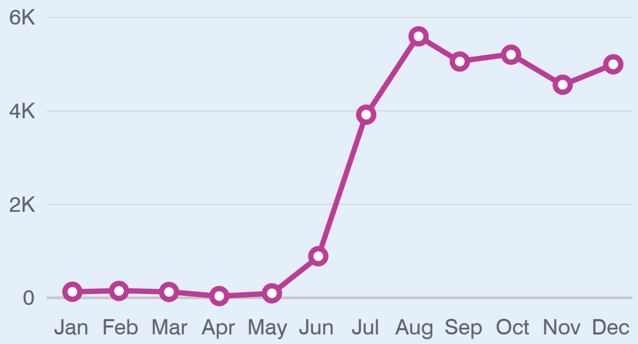
PROFILE OF A FAST-GROWING TLD

For many of the fastest-growing TLDs, growth in new registrations correlated with an increase in registrars offering those TLDs. For example, monthly registrations of ".services" increased from 123 to 4,911 between January and December. During the same period, the number of registrars selling ".services" domains more than doubled from 24 to 55. The cheapest price for the TLD also fell from nearly $8 to less than $2 during this time. A similar pattern occurs for many of the fastest-growing TLDs.

Registrars for ".services"



Registrations for ".services"



KEYWORD PAIRS

Domains feature a variety of words and phrases. We tracked the most common English-language word pairs in 2018 domain registrations. Some pairs consistently appeared in the top thirty rankings, including "real estate," U.S. city names, and cryptocurrency-related terms.

Even so, keyword pair trends also demonstrated the same fluidity as other domain elements such as TLDs. In April, for example, vacation-themed keyword pairs were registered in high quantities. Car-related keyword pairs also surged during the spring.

We also observed a range of technology-related keyword pairs throughout the year, though exact phrases varied from month to month. These pairs often included terms such as "server," "security," and "system."

Top Keyword Pairs in 2018

1. real estate
2. for sale
3. i am
4. new york
5. bit coin
6. how to
7. i love
8. make up
9. block chain
10. web design
11. for you
12. we are
13. las vegas
14. to do
15. san diego
16. house of
17. the best
18. the world
19. move is
20. los angeles

Table 3

Top Keyword Pairs by Month

RANK	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
1	scoop to	instant winner	real estate	all inclusive	zen desk	real estate	real estate	real estate	real estate	real estate	real estate	real estate
2	facts to	i love	info to	inclusive vacation	intercom mail	for registration	apple id	block chain	for sale	casual meetings	bit coin	for sale
3	info to	real estate	facts to	real estate	secure server	the queue	bit coin	security check	how to	go out	i am	i am
4	wisdom to	star games	scoop to	new car	femme cougar	available for	for sale	check version	i am	out together	a flash	new york
5	insight to	how to	wisdom to	inclusive vacations	sexe femme	release from	how to	i am	bit coin	block chain	block chain	bit coin
6	going ahead	applicatio and	insight to	new cars	new car	queue available	i am	bit coin	new york	i am	for sale	how to
7	moving ahead	i phone	for sale	to own	car spanish	after release	resort living	server not	make up	for sale	new york	block chain
8	to save	my best	new york	rent to	us courts	to do	for you	not responding	i love	bit coin	how to	i love
9	to own	safe systems	how to	how to	a host	for sale	new york	for sale	for you	a flash	we are	make up
10	to have	bit coin	for you	walk in	cyber monday	how to	make up	apple id	las vegas	how to	for you	web design

Figure 9

FRAUDULENT DOMAINS

Across the fraudulent domains registered in 2018

95%	resolve to an IP address
94%	have an HTTP response
16%	have an MX record
26%	have a security certificate

Most domains are registered by businesses and individuals for legitimate purposes. But fraudsters also register millions of domains each year. These include fraudulent domains used to launch phishing attacks, lookalike or "typosquatting" domains that capitalize on unintentional traffic intended for other sites, and domains used to sell knockoff goods or scam customers. In addition to registering new domains for fraudulent purposes, fraudsters often exploit existing legitimate domains. Points of transition in a legitimate domain's life cycle, including expiration and deletion, present an opportunity for fraudsters to take over, often undetected. Businesses across industries are undermined by fraudulent domains.

Between Q1 and Q4, our data indicates that registrations of fraudulent domains rose 11%

We classify domains as fraudulent using a proprietary classification engine that analyzes domain records, website content, email activity, reputation and other dynamic factors.

Fraudulent domains resolve to IP addresses and have HTTP responses at a much higher rate than domains overall. They are also more likely to have a security certificate.

TLD TRENDS

Figure 10 shows the top TLDs used in fraudulent domain registrations. Research by Spamhaus recently highlighted several TLDs as "shady," based on the percentage of websites with specific TLDs conducting spam operations.[5] Several of these "shady" TLDs appear in the list of top TLDs for fraudulent domain registrations as well.

For example, ".top" is No. 2, ".men" is No. 19, and ".work" is No. 50. But threat actors are using more "innocuous" TLDs than "shady" TLDs. This includes several European country code TLDs. In the wake of GDPR, some of the European country code TLDs were the first to redact WHOIS information, which may have made them attractive to fraudsters.

Because the success of fraudulent domains depends on tricking people, hiding in plain sight can prove effective. As with suspicious IP addresses, this ambiguity makes identifying fraudulent domains difficult based on one factor alone.

Top TLDs for Fraudulent Domains

1.	.com	38%	6.	.РФ	3%
2.	.top	12%	7.	.xyz	2%
3.	.fr	8%	8.	.us	2%
4.	.co.uk	6%	9.	.org	1%
5.	.it	5%	10.	.net	1%

Table 4

Top TLDs Registered by Month

RANK	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
1	com	com	com	com	com	com	top	com	com	com	com	com
2	fr	fr	fr	fr	top	top	com	top	top	fr	xyz	top
3	it	РФ	it	it	fr	fr	co.uk	co.uk	co.uk	РФ	fr	fr
4	co.uk	co.uk	co.uk	xyz	it	it	fr	fr	fr	xyz	РФ	РФ
5	РФ	it	РФ	top	co.uk	co.uk	it	it	it	co.uk	site	xyz
6	org	org	org	co.uk	us	ooo	РФ	xyz	xyz	site	online	co.uk
7	top	us	ca	РФ	app	РФ	net	us	РФ	top	club	club
8	se	net	ru	org	org	net	ca	РФ	online	online	ru	ru
9	xyz	xyz	net	net	men	us	club	online	ca	se	se	net
10	ru	ru	se	pl	РФ	org	us	club	us	club	net	se

Figure 10

[5] Spamhaus. "The World's Most Abused TLDs." Accessed April 2019.

REGISTRARS

Fraudulent domains used many of the same registrars as legitimate ones. Some registrars, however, are more popular for fraudulent domain registrations. NameSilo, which appears as No. 2 in Table 5, accepts payment in Bitcoin and offers free WHOIS privacy for registrants. This anonymity likely makes the registrar an attractive choice for fraudsters.

Top Registrars for Fraudulent Domains

1.	Chengdu west dimension digital	14%
2.	NameSilo, LLC.	11%
3.	PDR Ltd. d/b/a PublicDomainRegistry.com	9%
4.	GoDaddy.com, LLC.	8%
5.	HOSTING CONCEPTS B.V.	6%
6.	NameCheap, Inc.	5%
7.	Gransy s.r.o d/b/a subreg.cz.	5%
8.	Alibaba Cloud Computing (Beijing) Co., Ltd.	4%
9.	Limited Liability Company "Registrar of domain names REG.RU"	3%
10.	Hosting Concepts B.V. d/b/a Openprovider	3%
11.	1API GmbH	2%
12.	DYNADOT, LLC	2%
13.	West263 International Limited.	2%
14.	Netim	2%
15.	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	2%
16.	1&1 Internet SE	1%
17.	Xin Net Technology Corporation.	1%
18.	Bizcn.com, Inc.	1%
19.	Regional Network Information Center, JSC dba RU-CENTER.	1%
20.	GMO	1%

IDN ATTACKS

Fraudulent IDN domains are poised for an attack

79% resolve to an IP address

75% have an HTTP response

49% have an MX record

16% have a security certificate

Internationalized domain names (IDN) allow people to use domain names in local, non-Latin languages and scripts. They are also are a common vehicle that threat actors use to create fraudulent domains. Many characters in alphabets such as Cyrillic look identical or nearly identical to characters in the Latin alphabet. By substituting them in place of corresponding Latin characters, attackers can create fake domains resembling popular brand domains.

Fraudulent IDN domains are a widespread problem. In 2018, nearly 66% of Proofpoint Digital Risk Protection customers had at least one detection for an active fraudulent IDN domain that uses their brand name. And for more than 1 in 5 of those customers, the fraudulent domains are almost an exact match for their brand-owned domain, with just one or two characters swapped.

Top Registrars for IDN Attacks

1.	Registrar of Domain Names REG.RU, LLC	21%
2.	GoDaddy.com, LLC.	13%
3.	1&1 Internet SE	12%
4.	GMO	6%
5.	Google Inc.	4%
6.	Regional Network Information Center, JSC dba RU-CENTER.	4%
7.	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	3%
8.	R01-RF.	2%
9.	OVH	2%
10.	Gandi SAS	2%
11.	NameCheap Inc.	2%
12.	Regtime Ltd	2%
13.	Loopia AB	1%
14.	BEGET-RF	1%
15.	TIMEWEB-RF	1%
16.	Internet Domain Service BS Corp.	1%
17.	Mesh Digital Limited	1%
18.	NETHOUSE-RF	1%
19.	Cronon AG.	1%
20.	Nics Telekomunikasyon Tic Ltd. Sti.	1%

Table 6

NEARLY **66%** of Proofpoint Digital Risk Protection customers had at least one detection for a fraudulent IDN in 2018

LOOKALIKE DOMAINS

Lookalike domains, too, are poised for an attack

79%	resolve to an IP address
73%	have an HTTP response
34%	have an MX record
17%	have a security certificate

To create a lookalike domain, fraudsters add or change as few characters as possible in the company's brand domain. These changes are often so subtle that they are difficult for visitors to detect. For example, the letter "m" can be replaced by the letters "r" and "n" to give the appearance of "m." In the case of acmeanvils.com, the lookalike domain would appear as in acrneanvils.com.

Our code-cracking brains naturally "autocorrect" these lookalike spellings to make sense of them. Attackers know this and exploit this tendency regularly.

Our data indicates that lookalike domain registrations increased 18% between Q1 and Q4 2018. And like IDN attacks, they represent a widespread concern.

Like fraudulent domains overall, lookalike domains hide in plain sight when it comes to TLDs and registrars:

76% of Proofpoint Digital Risk Protection customers had at least one detection for a lookalike domain in 2018

Top TLDs for Lookalike Domains

1.	.com	42%
2.	.net	5%
3.	.ru	5%
4.	.org	3%
5.	.info	3%
6.	.xyz	3%
7.	.top	3%
8.	.online	2%
9.	.cn	2%
10.	.club	2%

Table 7

Top Registrars for Lookalike Domains

1.	GoDaddy.com, LLC	23%
2.	NameCheap, Inc.	9%
3.	Alibaba Cloud Computing (Beijing) Co., Ltd.	5%
4.	Registrar of Domain Names REG.RU, LLC	4%
5.	PDR Ltd. d/b/a PublicDomainRegistry.com	4%
6.	Tucows Domains Inc.	3%
7.	GMO Internet, Inc. dba Onamae.com	3%
8.	Xin Net Technology Corporation	2%
9.	NameSilo, LLC	2%
10.	Name.com, Inc.	2%
11.	Google Inc.	2%
12.	DYNADOT, LLC	2%
13.	eNom, Inc.	2%
14.	Network Solutions, LLC	2%
15.	Chengdu West Dimension Digital Technology Co., Ltd.	2%
16.	Regional Network Information Center, JSC dba RU-CENTER	1%
17.	OVH	1%
18.	1&1 Internet SE	1%
19.	123-Reg Limited	1%
20.	Domain.com, LLC	1%

Table 8

TLD ATTACKS

75% resolve to an IP address

70% have an HTTP response

37% have an MX record

13% have a security certificate

TLD attacks are exact matches of the brand domain with different endings after the “dot.” For example, if the brand-owned domain was acmeanvils.com, threat actors might register acmeanvils.gq or acmeanvils.work.

Whitehouse.com is a famous example of this domain type. In 1997, Dan Parisi seized on this TLD opportunity and purchased the “whitehouse.com” domain. He then turned it into a pornography site that generated $1 million in revenue per year.

The official domain of the White House is whitehouse.gov. Although .gov as a TLD is only available to official government sites, it is more common for people to type the .com TLD. In this case, that simple “com” typo would land users on an adult site by mistake. Because of the explicit and commercial content of the site, it is frequently cited as one of the most egregious examples of TLD domain misuse.

Because the most popular TLDs (“.com” and “.net”) are unavailable, TLD attacks use a more broadly distributed set of TLDs than other types of fraudulent domains. In the chart below, note the appearance of .app and .icu, which are new TLDs launched in 2018. Fraudsters pay attention to new TLD releases and rush to register brand names with them as quickly as possible.

TLD attack domain characteristics also show higher active resolutions than we see in the broader domain universe

TLD attacks affect nearly all enterprises:

96%+ of Proofpoint Digital Risk Protection customers had at least one TLD attacks detection in 2018.

23% TLD attack registrations increased between Q1 and Q4 of 2018

Top TLDs for TLD Attacks

1.	.app	6%
2.	.ooo	3%
3.	.xyz.	3%
4.	.online	2%
5.	.site	2%
6.	.club	2%
7.	.top	2%
8.	.info	2%
9.	.icu	2%
10.	.website	1%

Table 9

Top Registrars for TLD Attacks

1.	GoDaddy.com, LLC.	17%
2.	NameCheap, Inc.	12%
3.	Alibaba Cloud Computing (Beijing) Co., Ltd.	10%
4.	PDR Ltd. d/b/a PublicDomainRegistry.com.	5%
5.	Tucows Domains Inc.	3%
6.	Google Inc.	3%
7.	Name.com, Inc	3%
8.	Dynadot LLC	2%
9.	Key-Systems LLC	2%
10.	Chengdu West Dimension Digital Technology Co., Ltd.	2%
11.	Uniregistrar Corp.	2%
12.	Network Solutions, LLC.	2%
13.	OVH	2%
14.	GMO Internet, Inc. d/b/a Onamae.com.	2%
15.	Gandi SAS.	1%
16.	Registrar of Domain Names REG.RU, LLC.	1%
17.	1&1 Internet SE	1%
18.	1API GmbH	1%
19.	NameSilo, LLC.	1%
20.	Regional Network Information Center, JSC dba RU-CENTER.	1%

Table 10

DOMAINS SELLING COUNTERFEIT GOODS

Some domains use a brand name and append words like “online,” “sale” or “outlet.” These domains lead to websites that entice customers with deep discounts and special pricing. Users are then tricked into providing their personal information and credit card numbers. If they actually receive an item purchased on these sites, the items are usually cheap knockoffs of the brand’s goods. In many cases, attackers simply steal the personal and payment information without ever shipping anything.

78% of retail brands had at least one detection in 2018 for domains selling counterfeit goods

On average, each of these customers had more than 200 detections. Businesses that sell high-value goods—for example, luxury fashion, watches or sneakers—experienced a much higher rate. Registrations of counterfeit domains increased 11% between Q1 and Q4 of 2018, spiking in Q3, likely in preparation for Q4 holiday shopping.

30% have security certificates

Domains selling counterfeit goods have security certificates at a significantly higher rate than other types of fraudulent domains. This likely reflects an effort to make their transactions appear more legitimate.

On the other hand, only 8% of counterfeit domains have MX records. This suggests that they mainly use other channels such as social media and sites with public comments enabled to drive traffic to their sites rather than email.

Top Registrars
For Domains Selling Counterfeit Goods

1.	Chengdu west dimension digital	18%
2.	NameSilo, LLC.	14%
3.	PDR Ltd. d/b/a PublicDomainRegistry.com [Tag = PDR-IN]	10%
4.	HOSTING CONCEPTS B.V.	8%
5.	Alibaba Cloud Computing (Beijing) Co., Ltd.	7%
6.	Gransy s.r.o d/b/a subreg.cz.	6%
7.	GoDaddy.com, LLC.	5%
8.	NameCheap, Inc	5%
9.	Hosting Concepts B.V. d/b/a Openprovider	3%
10.	1API GmbH	3%
11.	DYNADOT, LLC	2%
12.	West263 International Limited.	2%
13.	Netim	2%
14.	Bizcn.com, Inc.	1%
15.	Xin Net Technology Corporation.	1%
16.	Xiamen 35.Com Technology Co., Ltd.	1%
17.	Registrar.eu	1%
18.	Web Commerce Communications Limited dba WebNic.cc	1%
19.	InterNetX GmbH	1%
20.	HEXONET Services Inc.	1%

Table 11

Top TLDs

For Domains Selling Counterfeit Goods

1.	.com	41%	6.	.xyz	2%
2.	.top	16%	7.	.us	2%
3.	.fr	9%	8.	.org	1%
4.	.co.uk	8%	9.	.ru	1%
5.	.it	6%	10.	.net	1%

Table 12

Top Security Certificate Issuers

For Domains Selling Counterfeit Goods

1.	COMODO CA Limited	43%
2.	Let's Encrypt	21%
3.	CloudFlare	20%*
4.	cPanel	14%
5.	TrustAsia Technologies	1%

Table 13

Top Web Servers

For Domains Selling Counterfeit Goods

1.	apache	67%
2.	cloudflare	23%*
3.	nginx	7%
4.	litespeed	0.7%
5.	wcsflareplus	0.7%

Table 14

Top Countries Hosting

For Domains Selling Counterfeit Goods

1.	United States	56%
2.	Netherlands	15%
3.	Turkey	8%
4.	Great Britain	6%
5.	Sweden	5%
6.	Estonia	3%
7.	Russia	1%
8.	France	0.6%
9.	Germany	0.6%
10.	Romania	0.4%

Table 15

Top Autonomous System Numbers (ASN)

For Domains Selling Counterfeit Goods

1.	13335-CLOUDFLARENET: Cloudflare, Inc., US	23%*
2.	41204-HOSTCOOL, NL	12%
3.	18779-EGIHOSTING: EGIHosting, US	7%
4.	36352-AS-COLOCROSSING: ColoCrossing, US	6%
5.	204353-GLOBALOFFSHORE, GB	5%
6.	59447-SAYFANET, TR	5%
7.	33387-NOCIX - DataShack, LC, US	4%
8.	64435-GREENBEI, SE	3%
9.	197328-INETLTD, TR	3%
10.	29073-QUASINETWORKS, NL	2%

Table 16

* Cloudflare is an anti-DDoS product (likely included by default by some hosting providers) and masks the name of the actual hosting provider and web server for some of these domains.

FRAUDULENT DOMAINS AND SECURITY CERTIFICATES

Websites with a security certificate start with "HTTPS" rather than "HTTP" and feature some type of padlock icon, depending on the web browser.

Not long ago, security awareness training taught users to look for the padlock symbol at the beginning of a URL to ensure a website was safe. But a security certificate does not mean the site has been validated as trusted or legitimate. It only signifies that the data transmitted between the user's browser and the site is encrypted and third parties cannot intercept and read the information in real time.

Our research found that cyber criminals use security certificates in **26%** of their domains

Security certificates increased over the course of 2018 from just over 12% to more than **27%**

Our research found that cyber criminals use security certificates in 26% of their fraudulent domains. This finding is especially concerning because all those years of "trust the padlock" training have led many internet users to perceive these sites as legitimate.

Top Issuers of Security Certificates for Fraudulent Domains

1.	COMODO CA Limited	39%
2.	Let's Encrypt	27%
3.	CloudFlare	18%
4.	cPanel	13%
5.	DigiCert Inc	1%

Table 17

As Figure 11 shows, the percent of newly registered fraudulent domains with security certificates increased over the course of 2018 from just over 12% to more than 27%. This increase (and the spike in July) was likely a response to Google's announcement that Chrome would begin warning users that sites without security certificates are "not secure." We expect the rate to continue climbing in 2019.

Fraudulent Domains with Security Certificates

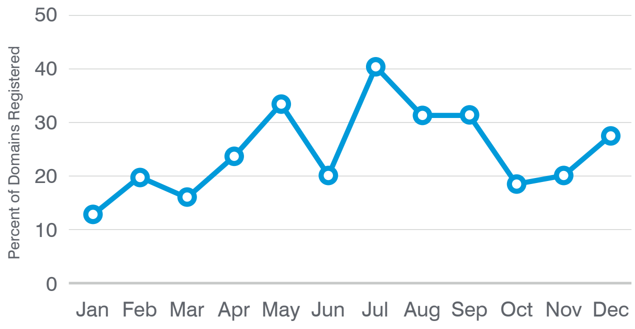


Figure 11

EMAIL TRENDS

Proofpoint email security products give our domain fraud analysts unique insight into enterprise email activity. This includes email traffic from fraudulent domains.

Fraudulent domains sending email were generally quick to act, with over 50% observed sending email within 30 days of registration. The full breakdown appears in Figure 12.

For most fraudulent domains sending email, we saw a low volume of activity. This points to highly targeted and socially engineered attacks such as a form of wire fraud known as business email compromise (BEC).

94% of Proofpoint Digital Risk Protection customers observed at least one of their fraudulent domain detections sending email in 2018.

50% observed sending email within 30 days of registration day

FRAUDULENT DOMAINS: TIME TO EMAIL ACTIVITY

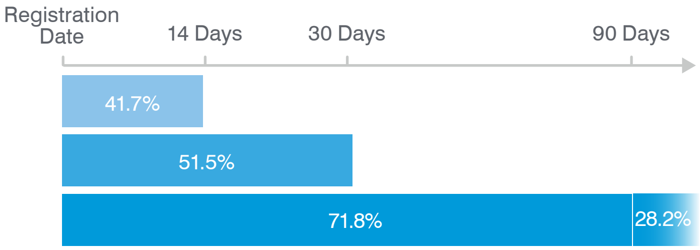


Figure 12

For 96% of fraudulent domains sending email, we saw fewer than 100 emails on the first date of email activity. For some fraudulent domains impersonating highly recognizable retail brands (especially those with complex supply chains), we observed much higher volumes of email, suggesting more broad-based attacks against customers and partners.

Some companies have successfully gained ownership of domains that were fraudulently impersonating them through the Uniform Domain-Name Dispute-Resolution Policy (UDRP). But we have also seen many fail to implement Domain-Based Message Authentication, Reporting and Conformance (DMARC) on those acquired domains. The lack of a strict DMARC policy published by a domain allows fraudsters to spoof that domain and continue sending fraudulent email as if they still owned it.

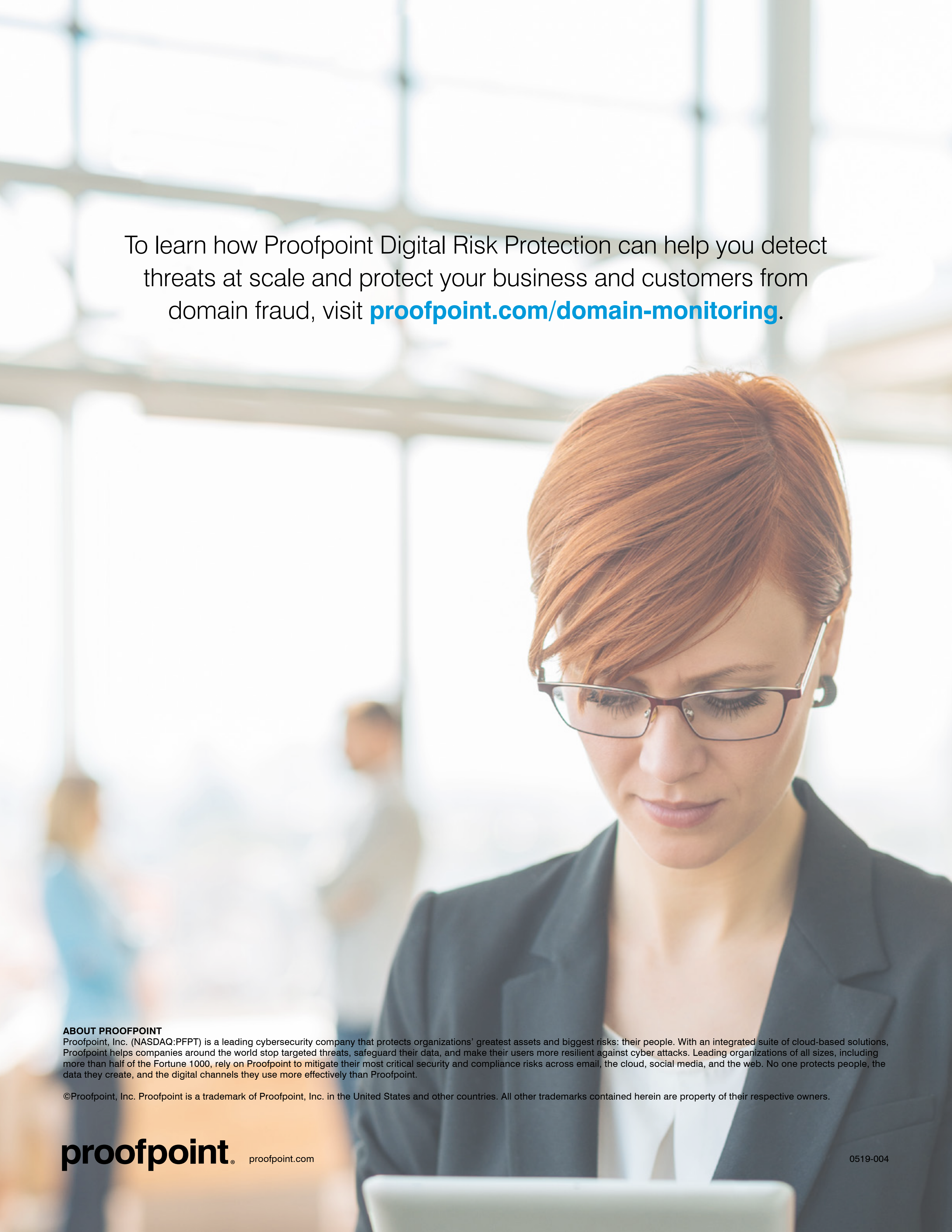
PARKED DOMAINS

“Parked” domains incorporate brand names and resolve to an “under construction” page or a page with advertisements. These domains are often owned and managed in bulk by “parking groups” and are not always used for malicious purposes such as phishing.

Still, “parked” domains are not harmless, either. At the very least, they monetize traffic intended for other businesses. At the worst, they may serve as indirect channels to malicious sites by redirecting traffic or may serve malicious ads.

91% of Digital Risk Protection customers had at least one detection for a “parking group” domain in 2018

The trend of “parked” domains appears to be on the rise. Registrations of “parking group” domains more than doubled between Q1 and Q4.



To learn how Proofpoint Digital Risk Protection can help you detect threats at scale and protect your business and customers from domain fraud, visit **proofpoint.com/domain-monitoring**.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.