PHISHING LANDSCAPE 2022

Greg Aaron
Interisle Consulting Group

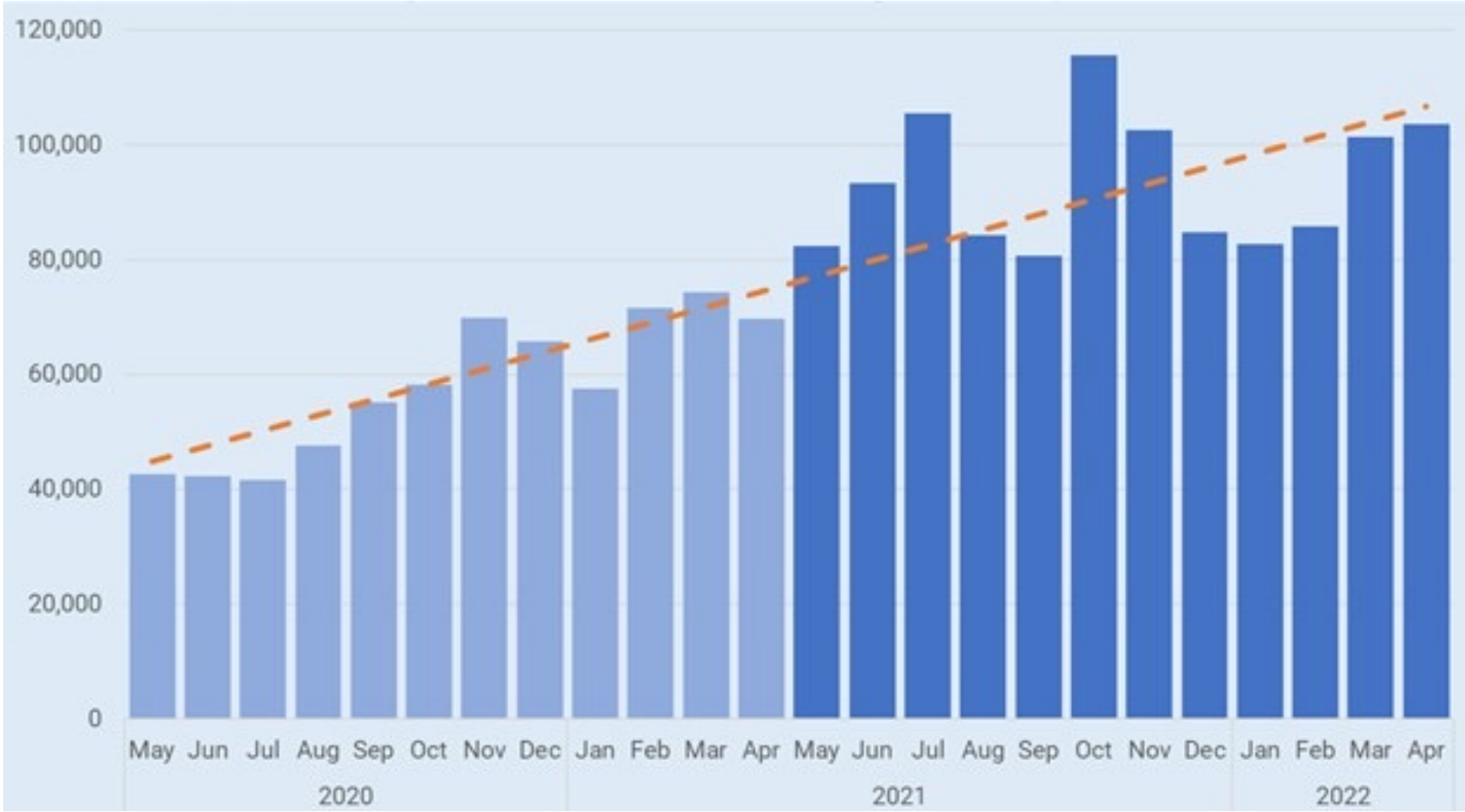
ICANN75

https://www.interisle.net/PhishingLandscape2022.html

One year of data: 1 May 2021 to 30 April 2022

1. data from widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. Only high-confidence reports.
2. More than 3 million phishing reports →
3. 1.1 million separate unique phishing attacks
4. 853,987 unique domain names used for phishing

NUMBER OF ATTACKS MORE THAN DOUBLED OVER TWO YEARS

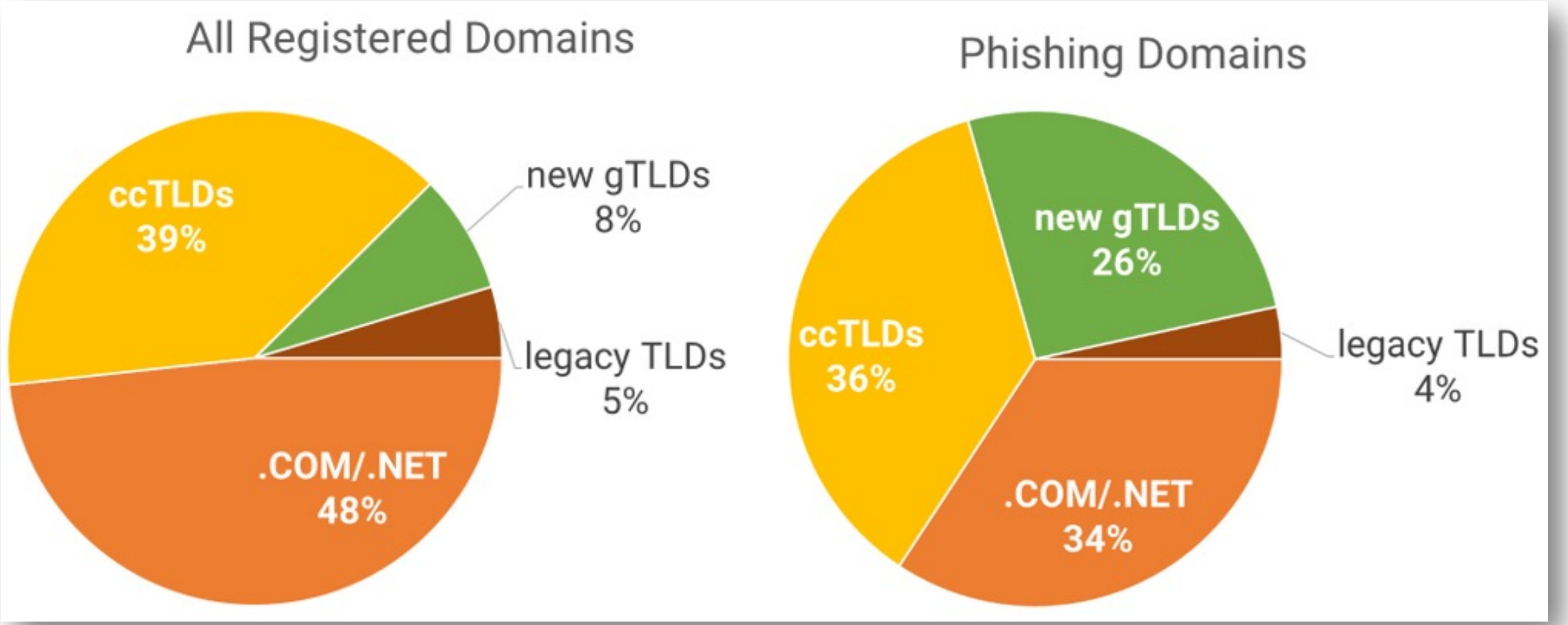


2022 Rank	TLD	Registry Operator	Domains in TLD	Phishing Domains Reported
1	com	Verisign	159,902,632	277,728
2	cn	CNNIC	8,980,611	103,869
3	shop	GMO Registry	1,040,404	47,747
4	xyz	XYZ.COM	4,130,573	38,604
5	tk	Freenom	5,041,535	37,300
6	ml	Freenom	5,344,979	28,318
7	ga	Freenom	7,049,929	25,717
8	cf	Freenom	5,383,367	17,747
9	bar	Punto 2012 SAPI	281,575	15,826
10	net	Verisign	13,170,783	15,083

56% OF GTLD DOMAINS USED FOR PHISHING WERE AT JUST 10 REGISTRARS:

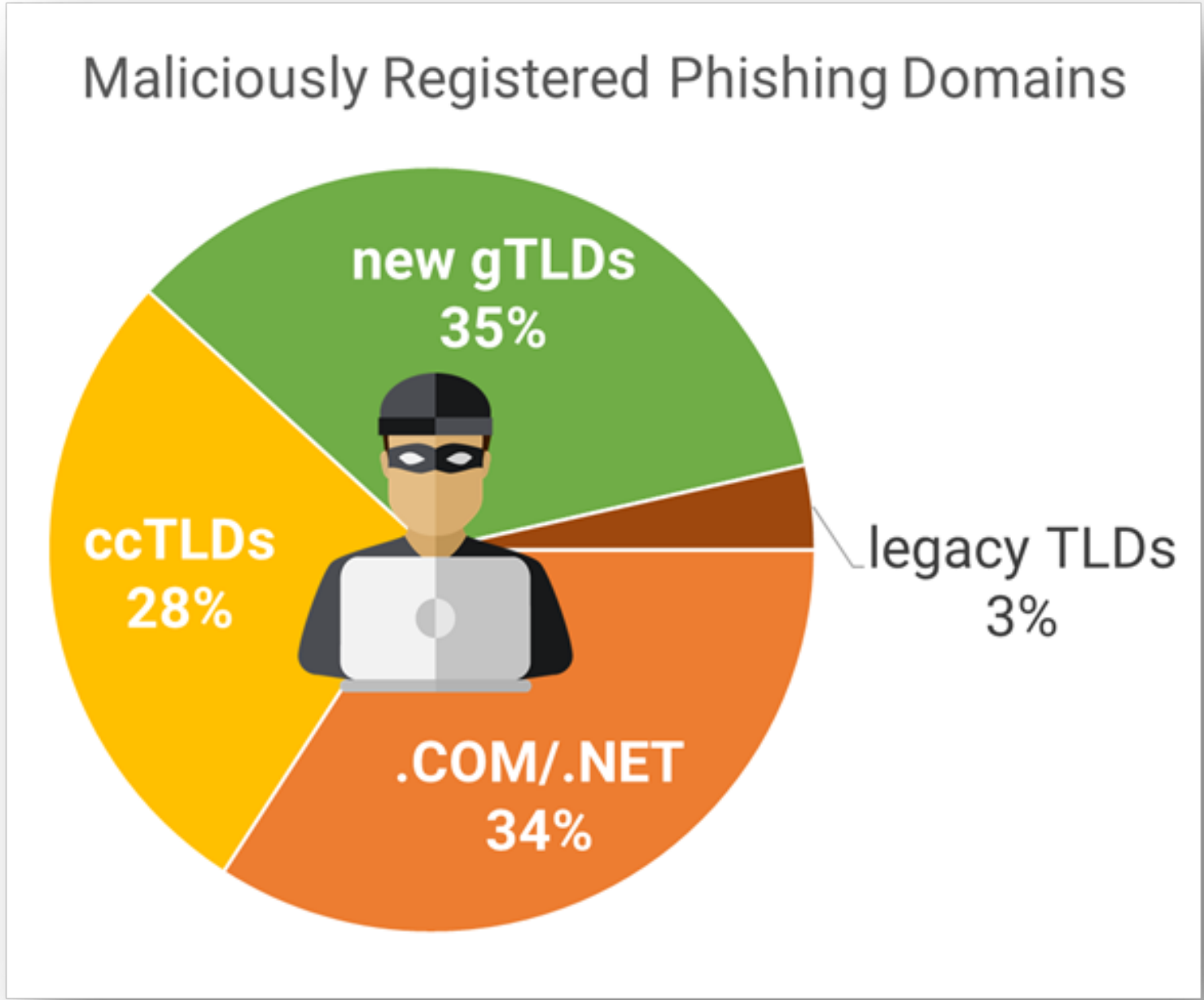
Rank	Registrar	Registrar IANA ID	gTLD Domains under Management	Phishing Domains Reported ▼
1	NameCheap	1068	13,645,340	**88,643**
2	GoDaddy.com	146	66,087,039	**44,160**
3	NameSilo	1479	4,403,551	**42,489**
4	DNSPod	1697	1,387,872	**30,778**
5	ALIBABA.COM SINGAPORE	3775	1,677,681	**27,538**
6	PublicDomainRegistry	303	4,916,665	**21,948**
7	REG.RU LLC	1606	726,674	**14,472**
8	Wild West Domains	440	2,962,240	**12,707**
9	Wix.com	3817	2,323,890	**11,287**
10	eNom	48	4,657,282	**10,101**

NEW GTLDS WERE 8% OF ALL REGISTERED DOMAINS, BUT 26% OF DOMAINS USED FOR PHISHING



MALICIOUSLY REGISTERED DOMAINS

1. **Most phishing occurs on domains registered by phishers**. 69% of domains used for phishing attacks were maliciously registered. (588,321 of the 853,987 domains reported for phishing in the study period.)
2. Most maliciously registered domains can be identified with high confidence. *(Quick use after registration; registrars have data.)*
3. Maliciously registered domains can/should be suspended by the registrar or registry operator, without risk of collateral damage.
4. The other 31% of phishing was on compromised domains (hacked servers/accounts), or on subdomain or other service providers. Here the provider must perform mitigation.


Maliciously Registered Phishing Domains
new gTLDs
35%
ccTLDs
28%
.COM/.NET
34%
legacy TLDs
3%

GTLDS WITH HIGH MALICIOUS REGISTRATIONS

TLD	Phishing Domains	Malicious Phishing Domain Registrations	Percent determined to be malicious ▼
bar	15,826	15,670	99%
work	10,315	10,150	98%
buzz	10,031	9,800	98%
shop	47,747	46,379	97%
xyz	38,604	35,665	92%
live	12,420	10,981	88%
top	14,758	12,498	85%
info	13,447	11,382	85%
com	277,727	191,660	69%
net	15,083	9,091	60%

SUBDOMAIN SERVICES

13% of phishing took place on subdomain services.

phish.domain.tld

domain	Owner
000webhostapp.com	Hostinger
blogspot.com	Google
trycloudflare.com	Cloudflare
duckdns.com	DuckDNS
My.id	PT Identitas Digital Nasional

38% OF ALL PHISHING ATTACKS WERE AT JUST TEN HOSTERS (ASN):

2022 Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing Attacks ▼
1	CLOUDFLARENET	13335	2,400,256	120,209
2	UNIFIEDLAYER	46606	1,207,808	63,510
3	MICROSOFT	8075	45,502,976	46,995
4	NAMECHEAP-NET	22612	102,912	40,969
5	GOOGLE	15169	23,099,904	30,397
6	AMAZON-02	16509	42,667,520	25,591
7	ALIBABA (US)	45102	4,955,136	24,242
8	QUADRANET-GLOBAL	8100	574,208	23,345
9	DIGITALOCEAN	14061	2,701,056	21,791
10	FASTLY	54113	457,728	20,541

HOSTS WITH HIGHEST PHISHING SCORES

Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing attacks	Phishing Attack Score ▼
1	NAMECHEAP-NET	22612	102,912	40,969	3980.97
2	CONTABO	40021	52,992	4,162	785.40
3	Domain names registrar REG.RU	197695	91,648	5,331	581.68
4	TimeWeb Ltd.	9123	59,136	3,147	532.16
5	UNIFIEDLAYER	46606	1,207,808	63,510	525.83
6	Hostinger International Limited	47583	124,672	6,278	503.56
7	CLOUDFLARENET	13335	2,400,256	120,209	500.82
8	INMOTI-1	54641	61,440	2,983	485.51
9	PONYNET	53667	63,232	3,061	484.09
10	FASTLY	54113	457,728	20,541	448.76

TAKE-AWAYS

1. *These numbers are a floor*. Phishing is under-reported and under-documented.
2. The majority of the problem is concentrated at small numbers of domain registrars, registries, and hosting providers.
3. Mitigation speed and *prevention* are critical.
4. Malicious domain name registrations are much of the problem. These can be identified. Registrars and registry operators can and should suspend them.