PHISHING LANDSCAPE 2021

Interisle Consulting Group
Greg Aaron, Lyman Chapin

https://www.interisle.net/PhishingLandscape2021.html

1. One year of data: 1 May 2020 to 30 April 2021
2. data from widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. Only high-confidence reports.
3. 1,487,914 phishing reports
4. 695,823 unique phishing attacks
5. 497,949 unique domain names used for phishing

REPORTED PHISHING UP NEARLY 70%

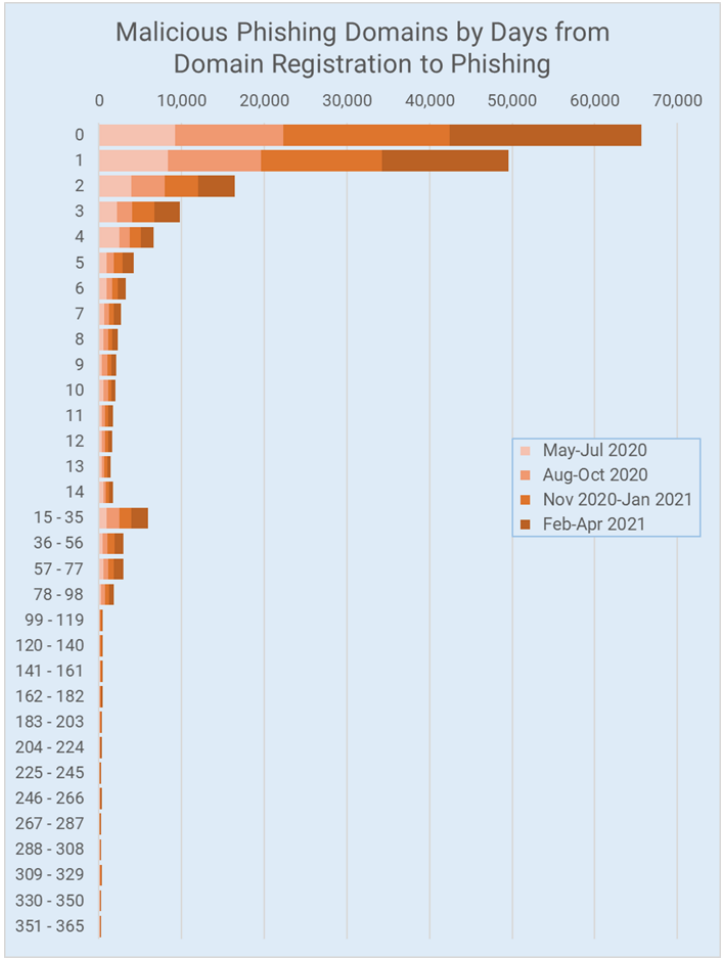
MALICIOUSLY REGISTERED DOMAINS

1. **Most phishing occurs on domains registered by phishers**. 65% of domains associated with phishing attacks were maliciously registered.
2. Maliciously registered domains can be suspended by the registrar or registry operator, without risk of collateral damage.
3. The other 35% of phishing was on compromised domains (hacked servers/accounts). Here the hosting provider can perform mitigation.

PHISHERS USE DOMAINS QUICKLY

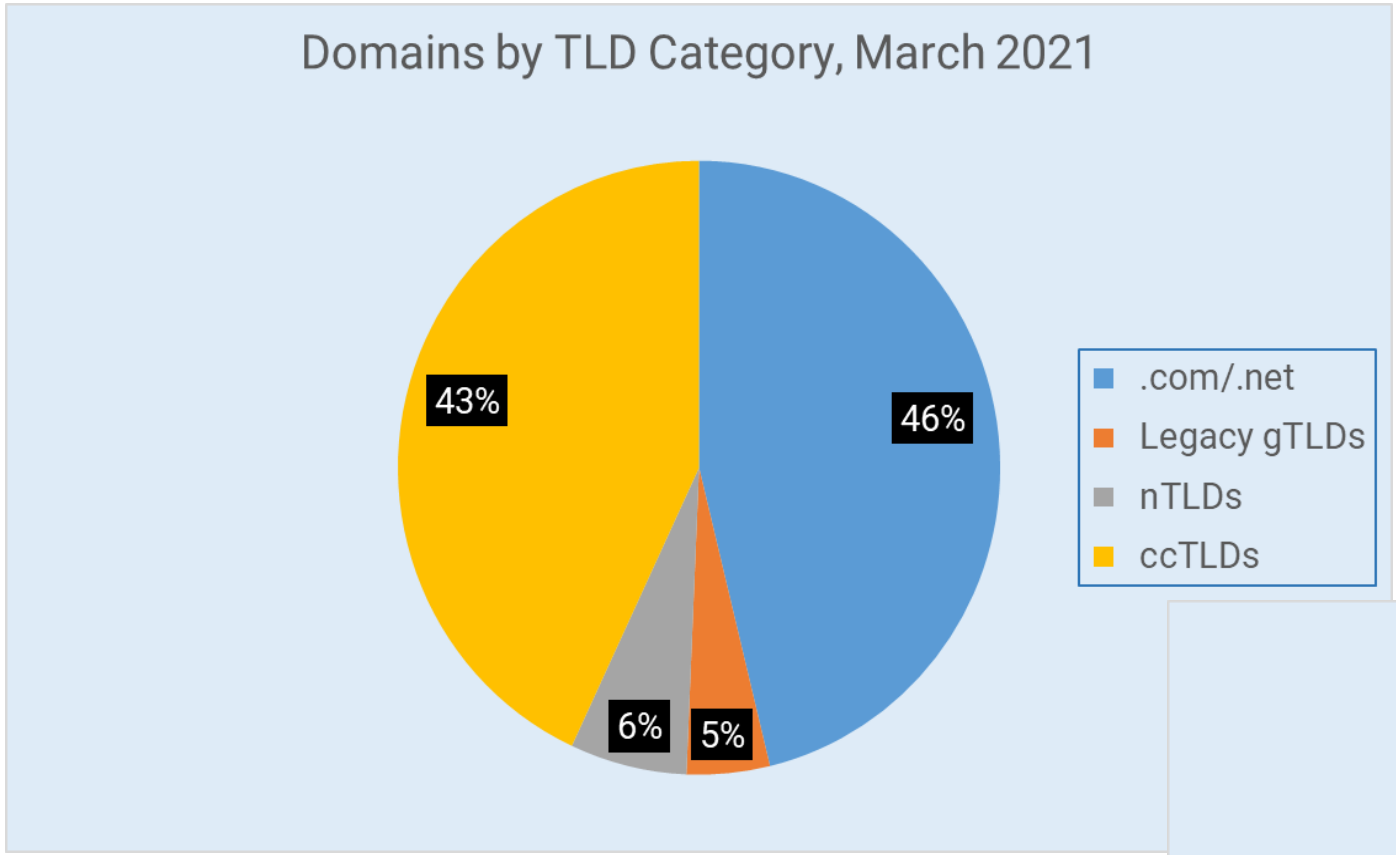
89% of maliciously registered domains are reported for phishing within 14 days following registration.

57% of domains reported for phishing were used within 14 days following registration. The majority of those were used within 48 hours of registration.

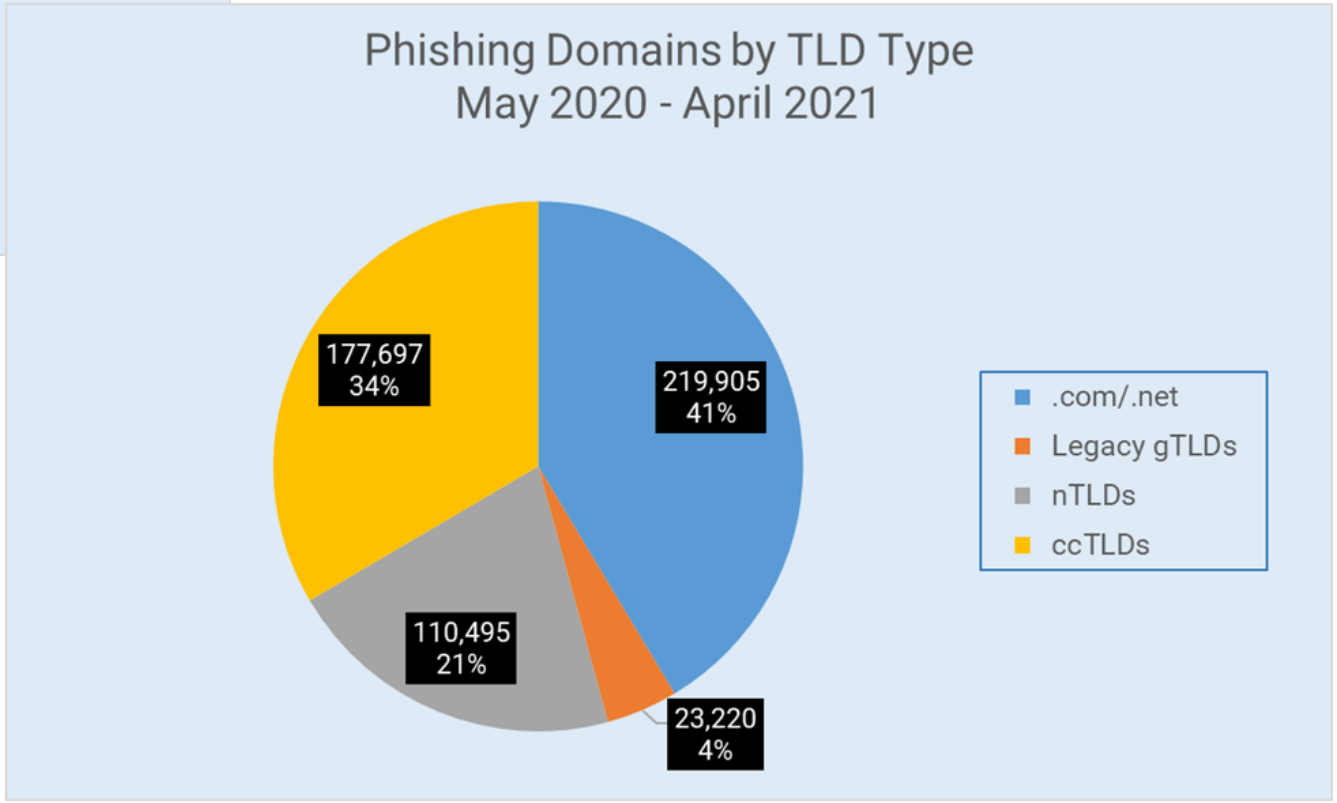


69% OF DOMAINS USED FOR PHISHING WERE IN JUST 10 TLDS:

Rank	TLD	Registry Operator	Domains in TLD	Phishing Domains Reported ▼
1	.com	Verisign	151,618,533	**260,636**
2	.tk	Freenom	19,987,952	**40,002**
3	.xyz	XYZ.COM	2,978,332	**27,532**
4	.ml	Freenom	3,816,199	**27,284**
5	.ga	Freenom	4,661,469	**21,657**
6	.cf	Freenom	4,179,760	**19,187**
7	.gq	Freenom	3,375,388	**16,168**
8	.cn	CNNIC	13,708,468	**16,052**
9	.top	Jiangsu Bangning	2,306,018	**15,129**
10	.net	Verisign	13,407,660	**14,398**



THE NEW GTLDS HAVE A MARKET SHARE OF 6%, BUT HAD 21% OF DOMAINS USED FOR PHISHING.



69% OF GTLD DOMAINS USED FOR PHISHING WERE AT JUST 10 REGISTRARS:

Rank	Registrar	Registrar IANA_ID	gTLD Domains under Management	gTLD Phishing Domains Reported ▼
1	NameCheap	1068	11,045,487	**79,118**
2	NameSilo	1479	3,501,471	**37,067**
3	GoDaddy.com	146	63,844,325	**35,150**
4	PublicDomainRegistry.com (PDR)	303	4,996,592	**19,065**
5	Tucows Domains	69	10,389,339	**9,972**
6	Wild West Domains	440	2,812,669	**8,582**
7	Google LLC	895	5,360,500	**8,413**
8	ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	3775	969,502	**7,883**
9	GMO Internet (Onamae.com)	49	5,000,613	**7,276**
10	eNom	48	5,171,823	**6,754**

MALICIOUS DOMAIN REGISTRATIONS (GTLDS):

Rank	Registrar	Malicious gTLD Domains Registrations
1	NameCheap	**60,629**
2	NameSilo	**28,105**
3	GoDaddy.com	**12,122**
4	PublicDomainRegistry.com (PDR)	**8,200**
5	Tucows Domains	**6,359**
6	Wild West Domains	**5,978**
7	Google	**5,679**
8	GMO Internet, Inc. (Onamae.com)	**5,394**
9	Name.com	**4,498**
10	Web Commerce Communications Limited (WebNic.cc)	**4,343**

41% OF ALL PHISHING ATTACKS WERE ON JUST TEN HOSTERS (ASN):

Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing Attacks ▼
1	NAMECHEAP-NET	22612	62,208	**55,903**
2	CLOUDFLARENET	13335	2,249,408	**52,011**
3	UNIFIEDLAYER-AS-1	46606	1,385,856	**35,363**
4	GOOGLE	15169	15,953,280	**32,330**
5	DIGITALOCEAN-ASN	14061	2,379,072	**15,794**
6	AWEX - Hostinger International Limited	204915	768	**13,186**
7	OVH - OVH SAS	16276	3,627,968	**12,604**
8	WEEBLY	27647	2,112	**10,701**
9	CONTABO - Contabo GmbH	51167	219,008	**10,635**
10	AMAZON-02	16509	41,090,304	**10,257**

TAKE-AWAYS

1. Phishing is a flourishing threat; number of attacks is high.
2. Most of the problem is concentrated at a small number of domain registrars, registries, and hosting providers.
3. Malicious domain name registrations are much of the problem. These can be identified, and registrars and registry operators should suspend them.