
CYBERSEC 2022 臺灣資安大會
CHANGE NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

ASM攻擊面管理和域名安全

台灣百大品牌企業之現狀與挑戰

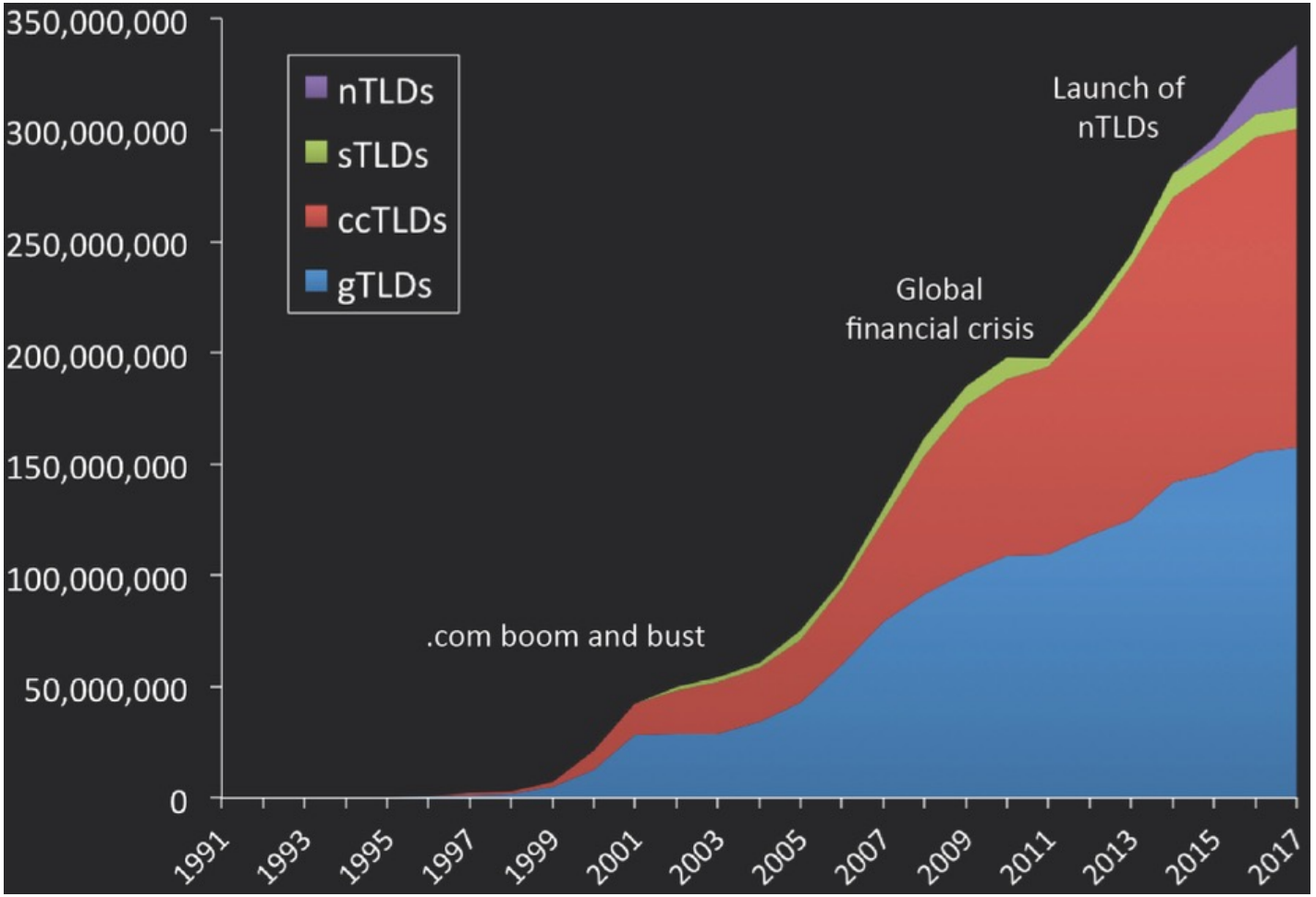
Sep–22–2022

喬敬 Ching Chiao

- WhoisXMLAPI 資深顧問 (2020~)
- TWNIC 數位品牌新頂級域名計畫 主持人 (2020~)
- 大點數據科技有限公司 創辦人/總經理 (2020~)
- 中域國際集團 創辦人/執行長 (2013~2020)
- Alibaba Group 集團顧問 (2010~2018)
- ICANN ccNSO 理事 (2014~2017)
- ICANN GNSO 理事 (2010~2014)
- TWIA 台灣網際網路協會 監事 (2007~)
- DotAsia (.asia) 註冊管理局董事 / 副總裁 (2006~2015)
- TWNIC 台灣網路資訊中心國際事務主管 (2003~2005)
- Register.com 亞太區業務經理 (2000~2002)

- 無論你是攻擊面管理（ASM）解決方案的提供商、網絡風險控制經理，還是滲透測試員，或是blue team成員，你需要全面瞭解你或你客戶 ASM 的情況。
- 企業面向網路的軟硬體資源越來越複雜，加上雲端服務、IoT設備的大量使用，帶給原本就難以彙整管理和監測的攻擊面，增加了大量盲點。
- 不論使用哪一個 ASM 工具，確保『全網可視性』是先決且必要的：廣泛而準確的數位資產掃描，包含***域名和子域名詳盡列舉***、***第三方應用服務發現***、 ***內外部IP地址之供應商以及地理資訊***等，以及其他關鍵性攻擊面查找與關聯分析。
- 及時獲取DNS相關數據，包括域名DNS、WHOIS、IP和其他網路數據和記錄等，有效地融入攻擊面情報中，能減少盲點的數量，提高攻擊面的預測性，有效管理潛在的攻擊與威脅因素。

ASM 工作重點	關鍵點
掃描、列舉並繪制完整的數位基礎設施	• 哪些域名使用了公司的郵件地址或其他註冊信息註冊的？它們會被用來做什麼? • 哪些子域名被添加到公司主要域名中? • 與6月、12月和24月前相比，今日的域名和子域名足跡有多大變化? • 這些域名解析到哪些IP地址？它們屬於哪些IP網塊/ISP?
創建雲服務/第三方服務庫	• 有多少域名、子域名和其他第三方所有的資產與一個特定的攻擊面相關? • 是否可通過DNS記錄或子域名識別第三方服務? • 機構的A記錄是否顯示了網絡集中而導致單點故障（SPoFs）？
發現內外部相關的依賴關係	• 在公司主要域名CNAME記錄中可發現哪些信息？是否有關第三方的技術細節? • 根據機構的MX記錄，誰是公司郵件服務器供應商? • 公司的子域名是否與懸空 (Dangling) DNS記錄有關?
實時監測惡意事件	• 是否存在針對公司各類商標、服務名稱、管理人員的域名冒充活動? • 是否存在利用域名生成算法（DGA）生成，被用作發起攻擊的網址? • 公司的IP地址是否被用於欺詐或惡意事件?



(Source: Zooknic, 2017)

Volume of Internet Infrastructure Data

Collected by WhoisXMLAPI

4.2 Billion+	721 Million+	20.7 Billion+
Domains and subdomains	Domains tracked historically	DNS records
15.6 Billion+	7,298+	99.5%
WHOIS records	TLDs & ccTLDs	of IP addresses in use
13.1 Million+	10,000+	11+
IP netblocks	Typosquatting domains added daily	Years of data crawling

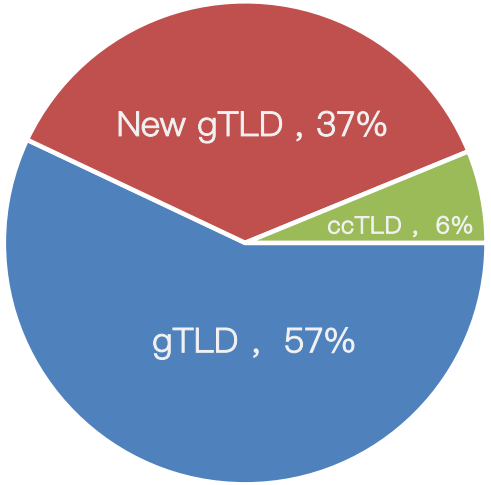
Apple

網域註冊總數

9,261

參考數字

Apple域名註冊種類

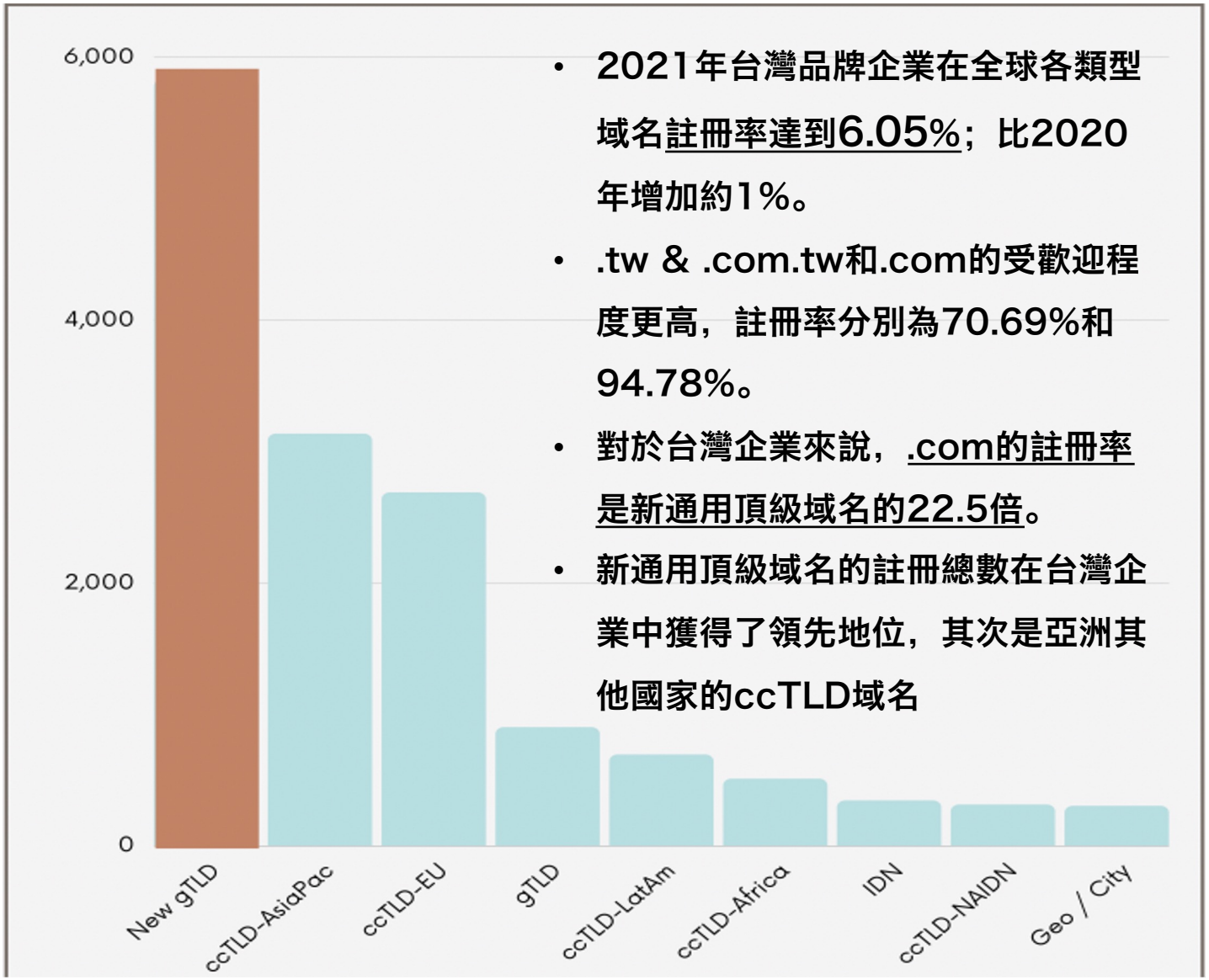


- ✓ 通用頂級域名（gTLD）5281個
- ✓ 國別域名（ccTLD）573個
- ✓ 新通用頂級域名（New gTLD）3407個
- ✓ 共涉及頂級域名類別共 379 個，其中 gTLD 8 個，ccTLD 54 個，New gTLD 317 個

新頂級域名建立台灣企業數位品牌識別度推廣計畫

https://gtld.tw

- 自2020年起由TWNIC發起的計畫
- 針對137家台灣上市企業以及經濟部Branding Taiwan 計畫輔導企業進行調查；訪談超過60家企業
- 持續追蹤各大品牌在全球 969 個 g + ccTLD 可供註冊之頂級域名上之註冊情形



- 2021年台灣品牌企業在全球各類型域名註冊率達到6.05%；比2020年增加約1%。
- .tw & .com.tw和.com的受歡迎程度更高，註冊率分別為70.69%和94.78%。
- 對於台灣企業來說，.com的註冊率是新通用頂級域名的22.5倍。
- 新通用頂級域名的註冊總數在台灣企業中獲得了領先地位，其次是亞洲其他國家的ccTLD域名

	A	B	C	D	E	F	G	H	I	J	K
1	New gTLD	ccTLD-EU	ccTLD-AsiaPa	gTLD	ccTLD-LatAm	IDN	ccTLD-Africa	Top4	Geo / City	ccTLD-NA	Total
2	140	93	88	23	22	17	14	11	11	9	428
3	asus.accounta	asus.am	asus.as	asus.biz	asus.ag	asus.世界	asus.cf	asus.com	asus.asia	asus.ca	
4	asus.app	asus.at	asus.az	asus.com	asus.ai	asus.中国	asus.cm	asus.icu	asus.moscow	asus.com.mx	
5	asus.asia	asus.ba	asus.cc	asus.info	asus.ar	asus.公司	asus.co.za	asus.top	asus.taipei	asus.mx	
6	asus.cam	asus.be	asus.cn	asus.jobs	asus.cl	asus.商标	asus.com.cm	asus.xyz	asus.广东	asus.us	
7	asus.cloud	asus.bg	asus.co.id	asus.mobi	asus.co	asus.广东	asus.com.tn	asuscomputer	rog.asia	rog.ca	
8	asus.club	asus.by	asus.co.il	asus.name	asus.com.ar	asus.网址	asus.gq	rog.com	rog.bayern	rog.com.mx	
9	asus.company	asus.ch	asus.co.in	asus.net	asus.com.br	asus.网络	asus.ma	rog.xyz	rog.lat	rog.mx	
10	asus.computer	asus.co.uk	asus.co.jp	asus.org	asus.com.co	rog.商标	asus.sh	zenbook.com	rog.moscow	rog.us	
11	asus.country	asus.com.es	asus.co.kr	asus.pro	asus.com.pe	rog.我爱你	asus.tn	zenbook.top	rog.rio	zenbook.us	
12	asus.cyou	asus.com.ge	asus.co.nz	asuscomputer	asus.uy	rog.网址	rog.cf	zenbook.xyz	rog.tokyo		
13	asus.email	asus.com.pl	asus.co.th	rog.com	rog.ai	华硕.中国	rog.co.za	华硕.com	华硕.广东		
14	asus.enterpris	asus.com.ua	asus.com.au	rog.info	rog.bz	华硕.企业	rog.mu				
15	asus.events	asus.cz	asus.com.cn	rog.jobs	rog.cl	华硕.商城	rog.org.za				
16	asus.faith	asus.de	asus.com.hk	rog.mobi	rog.co	华硕.广东	zenbook.co.za				
17	asus.family	asus.dk	asus.com.kz	rog.name	rog.com.br	华硕.我爱你					
18	asus.fans	asus.ee	asus.com.mv	rog.net	rog.com.ni	华硕.手机					
19	asus.feedback	asus.es	asus.com.my	rog.org	rog.gy	华硕.网址					
20	asus.fun	asus.eu	asus.com.np	zenbook.com	rog.pe						
21	asus.gallery	asus.fi	asus.com.ph	zenbook.jobs	rog.vc						
22	asus.game	asus.fr	asus.com.pk	zenbook.net	zenbook.cl						
23	asus.gay	asus.ge	asus.com.sa	zenbook.org	zenbook.co						
24	asus.gmbh	asus.gg	asus.com.sg	华硕.com	zenbook.com.br						
25	asus.group	asus.gr	asus.com.tr	华硕.net							
26	asus.host	asus.hr	asus.com.tw								
27	asus.icu	asus.hu	asus.hk								
28	asus.ink	asus.ie	asus.id								
29	asus.life	asus.im	asus.in								
30	asus.link	asus.it	asus.io								
31	asus.live	asus.lt	asus.ir								
32	asus.ltd	asus.lu	asus.jp								
33	asus.market	asus.lv	asus.kg								

Source: TWNIC 2021數位品牌調查

Typosquatting

com	top	icu	xyz
9999	241	116	950
asusasus.com	asusw.top	asuss.icu	susasusasusasusa.xyz
asus-asus.cor	asusr.top	asust.icu	asusasus.xyz
asuspegasus.(	asuss.top	aasus.icu	sorasusorasusorasusorasu.xyz
susasusasusa	asusn.top	easus.icu	asusu.xyz
dasusmatrasu	iasus.top	sasus.icu	rasus.xyz
pegasuspega:	asusu.top	paasus.icu	gasus.xyz
pegasusvega:	nasus.top	asussa.icu	asusp.xyz
asuš.com	dasus.top	asuspe.icu	sasus.xyz
asus-routeras	casus.top	asussc.icu	1asus.xyz
asüs.com	aasus.top	masuse.icu	pasus.xyz
lasus.com	sasus.top	oiasus.icu	casus.xyz
nasus.com	masus.top	aaasus.icu	asusa.xyz
uasus.com	hasus.top	asushr.icu	kasus.xyz
asusg.com	lasus.top	asusfa.icu	asust.xyz
asus2.com	csasus.top	asusxp.icu	nasus.xyz
asusu.com	asuser.top	asusga.icu	asusvr.xyz
masus.com	asushr.top	asus800.icu	asustv.xyz
asusn.com	asustv.top	asusscu.icu	asuszz.xyz
basus.com	zasush.top	kaasuss.icu	sobakasusobakasusobakasusobakasu.xyz
fasus.com	iasusr.top	wtasusv.icu	casusa.xyz
3asus.com	vasuse.top	asuslxy.icu	adasus.xyz
asuso.com	waasus.top	wasuser.icu	gasuse.xyz
asusp.com	ckasus.top	aasusue.icu	i-asus.xyz
asus8.com	dasush.top	asusraz.icu	goasus.xyz
asusv.com	rasush.top	alphasus.icu	kasusd.xyz
easus.com	asusvr.top	acerasus.icu	asusid.xyz
iasus.com	masusg.top	cnasusah.icu	asuspc.xyz

TldTags | Whois | Top4 | Subdomain Discovery | Typo

	domain-name	dns-a	dns-aaaa	dns-ns	dns-mx	geoip-country
original*	asus.com	103.10.4.216		ns1.edgecastdns.net	mg.asus.com	Taiwan
addition	asusa.com	219.118.222.245		dns1.asusa.net	asusam.asj-hosting.net	Japan
addition	asusb.com	199.59.242.153		ns1.bodis.com	mx76.m2bp.com	United States
addition	asusc.com	96.45.82.246		ns10.demosphere.com	mailstore1.secureserver.net	United States
addition	asusd.com	192.185.36.117		ns8185.hostgator.com	asusd.com	United States
addition	asuse.com	198.58.118.167		ns1.mytrafficmanagement.com		United States
addition	asusg.com	142.4.16.11		ns21.domaincontrol.com	asusg-com.mail.protection.outlook	United States
addition	asush.com	3.223.115.185		nsg1.namebrightdns.com		United States
addition	asusi.com	184.168.131.241		ns35.domaincontrol.com		United States
addition	asusl.com	45.121.197.59		ns1.dnshosting.hk	fosse.virtualhosting.hk	Hong Kong
addition	asusm.com		!ServFail			
addition	asusn.com	108.177.161.108		dm1.dns.com		United States
addition	asuso.com			ns1.namebrightdns.com		
addition	asusp.com	13.248.196.204				United States
addition	asusr.com	3.223.115.185		nsg1.namebrightdns.com		United States
addition	asuss.com	72.52.179.174		ns1.parklogic.com	mx156.hostedmxserver.com	United States
addition	asust.com	66.45.246.141				United States
addition	asusu.com	103.224.182.223		ns1.above.com	park-mx.above.com	Australia
addition	asusv.com			dns21.hichina.com	mxn.mxhichina.com	
addition	asusw.com		!ServFail			
addition	asusx.com	34.102.136.180		ns09.domaincontrol.com	alt1.aspmx.l.google.com	United States
addition	asusy.com	69.172.201.153		ns1.uniregistrymarket.link	mx247.in-mx.com	United States
bitsquatting	csus.com	205.178.189.131		ns39.worldnic.com	alt1.aspmx.l.google.com	United States
bitsquatting	esus.com	144.76.6.247		ns1.whizzit.com	us2.mx1.mailhostbox.com	Germany
bitsquatting	isus.com	47.90.30.95				Hong Kong
bitsquatting	qsus.com	91.195.241.136		ns1.sedoparking.com	localhost	Germany
bitsquatting	arus.com	184.173.24.78		dns101.register.com	arus2016.arus.com	United States
bitsquatting	aqus.com	151.139.128.10		ns1.appliedi.net	alt1.aspmx.l.google.com	United States
bitsquatting	awus.com	91.195.241.136		ns1.sedoparking.com	localhost	Germany
bitsquatting	acus.com	12.111.225.63		cbru.br.ns.els-gms.att.net	mxa-00191d01.gslb.pphosted.com	United States
bitsquatting	a3us.com	23.236.62.147		ns4.wixdns.net	a3us-com.mail.protection.outlook.c	United States
bitsquatting	asts.com	208.91.197.27		ns95.worldnic.com		United States
bitsquatting	asws.com	35.186.238.101		ns1.smartname.com		United States
bitsquatting	asqs.com	34.206.12.234		ns3.afternic.com		United States

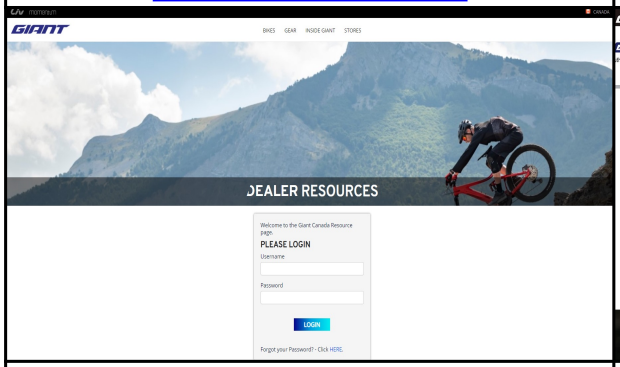
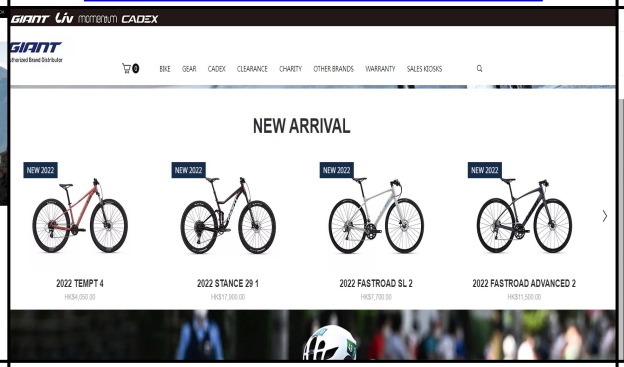
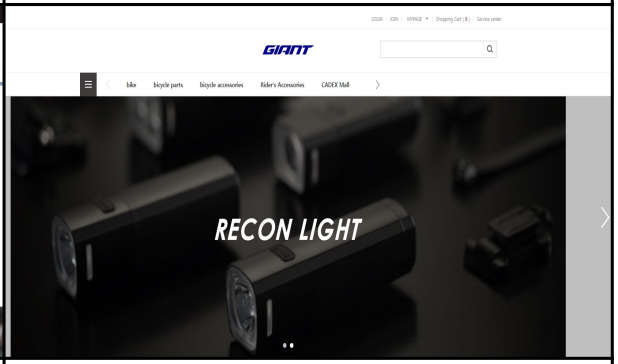
Source: TWNIC 2021數位品牌調查

巨大機械

多個官網入口 由不同註冊服務機構 **(Registrar)** 提供服務

網路中文	Enom	Realtime Register B.V.
www.giantgroup-cycling.com/	www.giantcyclingworld.com/	www.giant-bicycles.com/global

官網？ 還是釣魚網站？

www.giantbicycle.ca/	https://en.giantbicyclehk.com/	http://giantbicycle.co.kr/
		
GoDaddy	GoDaddy	Registrant: locajw@gmail.com

Semiconductor Brands

Brand name	Business domain	Research string	Domains added since August 16, 2020	Subdomains added since August 16, 2020
TSMC	tsmc.com	Starts with "tsmc."	18	14
UMC	umc.com	Starts with "umc."	26	61
Micron	micron.com	Starts with "micron."	28	40
AMD	amd.com	Starts with "amd."	55	213
Intel	intel.com	Starts with "intel."	31	163
NXP	nxp.com	Starts with "nxp."	12	44
GLOBALFOUNDRIES	gf.com	Starts with "gf."	40	892
SMIC	smics.com	Starts with "smics"	14	15
Broadcom	broadcom.com	Starts with "broadcom"	57	109
Nvidia	nvidia.com	Starts with "nvidia"	325	404
Qualcomm	qualcomm.com	Starts with "qualcomm"	67	102
MediaTek	mediatek.com	Starts with "mediatek"	95	125
SKHynix	skhynix.com	Starts with "skhynix"	28	8
Powerchip	powerchip.com	Starts with "powerchip"	16	1
Renesas	renesas.com	Starts with "renesas"	39	81
Infineon	infineon.com	Starts with "infineon"	60	120
MagnaChip	magnachip.com	Starts with "magnachip"	10	1
STMicro	st.com	Starts with "STMicro" (note: "st." involved over 5,000 subdomains)	69	77
TexasInstruments	ti.com	Starts with "TexasInstruments" (note: "ti." overly generic)	29	11
SamsungElectronics	semiconductor.samsung.com	Contains "semiconductor" + "samsung"	2	2

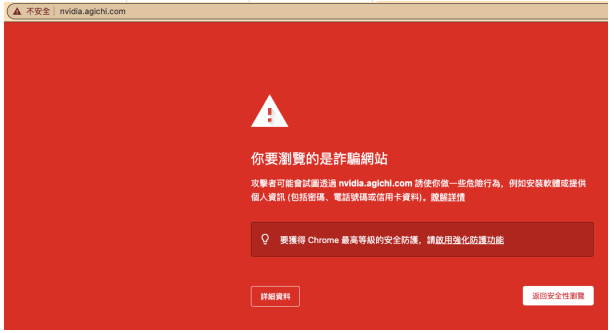
Nvidia: Domain and Subdomain discovery

nvidia-forum.ru	BEGET-RU		whois.ripn.net	ns1.beget.com|n	2021-12-25T12:17:13Z	2022-12-25T12:	2021-12-25 12:17:13 UTC	2022-12-25 12:1	REGISTERED,
nvidia-control-pa	NAMECHEAP IN	reactivation-pen	whois.namecheap.com	dns101.registrar	2021-07-21T09:	0001-01-01T00:	2022-07-21T09:	2021-07-21 09:2	0001-01-01 00:0	2022-07-21 09:2	clientTransferPr
nvidia-download	HOSTING CON	info@privacypro	whois.nic.fr	ns1.openprovide	2022-02-26T14:	2022-02-28T15:	2023-02-26T14:	2022-02-26 14:5	2022-02-28 15:1	2023-02-26 14:5	ACTIVE
nvidia-corp.net	Google LLC	registrar-abuse@	whois.google.com	NS-CLOUD-A1.(	2022-07-11T16:	2022-07-11T16:	2023-07-11T16:	2022-07-11 16:4	2022-07-11 16:4	2023-07-11 16:4	clientTransferPr
nvidia-abya.com	GoDaddy.com, L	abuse@godaddy	whois.godaddy.com	NS37.DOMAINC	2022-03-24T01:	0001-01-01T00:	2023-03-24T01:	2022-03-24 01:4	0001-01-01 00:0	2023-03-24 01:4	clientTransferPr
nvidia-docker.us	Gandi SAS	e620239256a6ff	whois.nic.us	ns-9-a.gandi.net	2022-01-21T08:	2022-01-26T08:	2023-01-21T08:	2022-01-21 08:1	2022-01-26 08:1	2023-01-21 08:1	clientTransferPr
nvidia-geforceno	Dattatec.com SF	abuse@donweb	whois.donweb.com	NS3.HOSTMAR	2022-05-14T21:	2022-05-19T21:	2023-05-14T23:	2022-05-14 21:5	2022-05-19 21:5	2023-05-14 23:5	ok
nvidia-inspector.	REGRU-SU	ms100m@yande	whois.ripn.net	ns1.sprinthost.ru	2022-01-26T11:48:06Z		2023-01-26T11:	2022-01-26 11:48:06 UTC		2023-01-26 11:4	REGISTERED,
nvidia-inspector.	TLD Registrar S	admin@tldregist	whois.eu	melany.ns.cloudflare.com|buck.ns.cloudflare.com|							
nvidia-geforceno	Dattatec.com SF	abuse@donweb	whois.donweb.com	NS3.HOSTMAR	2022-05-14T21:	2022-05-19T21:	2023-05-14T23:	2022-05-14 21:5	2022-05-19 21:5	2023-05-14 23:5	ok
nvidia-inspector.	123-Reg Limited	abuse@domaint	whois.123-reg.co.uk	DNS1.NAMECH	2022-03-22T21:	2022-08-04T13:	2023-03-22T21:	2022-03-22 21:2	2022-08-04 13:4	2023-03-22 21:2	ok
nvidia-flash.com	Registrar of dom	NVIDIA-FLASH.(	whois.reg.com	ns1.hosting.reg.(	2021-09-28T00:	2021-09-28T00:	2022-09-28T00:	2021-09-28 00:1	2021-09-28 00:1	2022-09-28 00:1	clientTransferPr
nvidia-offer.shop	Namecheap, Inc	abuse@namech	whois.namecheap.com	DNS1.REGISTR	2022-03-11T00:	2022-04-05T07:	2023-03-11T23:	2022-03-11 00:3	2022-04-05 07:1	2023-03-11 23:5	clientTransferPr
nvidia-offers.sho	Namecheap, Inc	abuse@namech	whois.namecheap.com	DNS1.REGISTR	2022-03-11T00:	2022-04-05T07:	2023-03-11T23:	2022-03-11 00:3	2022-04-05 07:1	2023-03-11 23:5	clientTransferPr
nvidia-profile-ins	REGRU-RU		whois.ripn.net	ns1.hosting.reg.(	2022-06-10T08:59:32Z		2023-06-10T08:	2022-06-10 08:59:32 UTC		2023-06-10 08:5	REGISTERED,
nvidia-meta.com	Alibaba Cloud C	DomainAbuse@	grs-whois.hichina.com	DNS23.HICHIN/	2021-11-25T17:	2022-03-25T02:	2022-11-25T17:	2021-11-25 17:2	2022-03-25 02:5	2022-11-25 17:2	ok
nvidia-geforceno	dattatec.com SR	nvidia-geforceno	whois.donweb.com	ns1.donweb.cl|n	2022-05-14T18:	2022-05-14T19:	2023-05-14T18:	2022-05-14 18:5	2022-05-14 19:0	2023-05-14 18:5	ok
nvidia-io.com	NAMECHEAP IN	854b087648314	whois.namecheap.com	dns1.registrar-se	2022-04-05T08:	0001-01-01T00:	2023-04-05T08:	2022-04-05 08:2	0001-01-01 00:0	2023-04-05 08:2	clientTransferPr
nvidia-global.cor	Internet Domain	nvidia-global.cor	whois.internet.bs	carter.ns.cloudfl	2022-08-03T15:	2022-08-03T16:	2023-08-03T15:	2022-08-03 15:4	2022-08-03 16:0	2023-08-03 15:4	clientTransferPr
nvidia-partner.co	007NAMES INC	abuse@007nam	whois.007names.com	ns1.007names.ri	2020-11-04T18:(	2021-09-08T19:	2022-11-04T18:(	2020-11-04 18:0	2021-09-08 19:5	2022-11-04 18:0	ok
nvidia-shops.ru	R01-RU		whois.ripn.net	ns1.fastfox.pro|n	2021-12-26T13:21:49Z		2022-12-26T13:	2021-12-26 13:21:49 UTC		2022-12-26 13:2	REGISTERED,
nvidia-reseach-n	ABOVE.COM PT	nvidia-reseach-n	whois.above.com	ns11.above.com	2022-03-03 08:0	2022-03-03 08:0	2023-03-03 08:0	2022-03-03 08:0	2022-03-03 08:0	2023-03-03 08:0	clientTransferPr
nvidia-technolog	REGRU-RU		whois.ripn.net	jean.ns.cloudflar	2022-06-29T07:32:52Z		2023-06-29T07:	2022-06-29 07:32:52 UTC		2023-06-29 07:3	REGISTERED,
nvidia-on-azure.(	GoDaddy.com, L	abuse@godaddy	whois.godaddy.com	NS57.DOMAINC	2021-08-12T16:	2022-08-13T12:	2023-08-12T16:	2021-08-12 16:1	2022-08-13 12:4	2023-08-12 16:1	clientTransferPr
nvidia-profile-ins	Registrar of dom	NVIDIA-PROFIL	whois.reg.com	ns1.hosting.reg.(	2022-06-10T08:	2022-06-10T08:	2023-06-10T08:	2022-06-10 08:5	2022-06-10 08:5	2023-06-10 08:5	clientTransferPr
nvidia-smi.icu	Alibaba Cloud C	domainabuse@a	grs-whois.hichina.com	DNS27.HICHIN/	2020-11-24T13:(	2022-02-06T18:	2022-11-24T23:5	2020-11-24 13:2	2022-02-06 18:3	2022-11-24 23:5	ok
nvidia-research-	GoDaddy.com, L	abuse@godaddy	whois.godaddy.com	NS1.BADGERD	2020-10-16T14:	2021-10-14T12:	2022-10-16T14:	2020-10-16 14:3	2021-10-14 12:2	2022-10-16 14:3	clientTransferPr
nvidia-softs.net	Registrar of dom	angelinaprohoro	whois.reg.com	ns1.firstbytedns.	2021-12-01T14:	2021-12-01T14:	2022-12-01T14:	2021-12-01 14:3	2021-12-01 14:3	2022-12-01 14:3	clientTransferPr
nvidia-sale.com	NAMECHEAP IN	reactivation-pen	whois.namecheap.com	dns101.registrar	2021-07-23T17:	0001-01-01T00:	2022-07-23T17:	2021-07-23 17:5	0001-01-01 00:0	2022-07-23 17:5	clientTransferPr
nvidia-stock.com	NAMECHEAP IN	84d3392b43814	whois.namecheap.com	ns11.cloudns.ne	2021-12-22T16:	0001-01-01T00:	2022-12-22T16:	2021-12-22 16:3	0001-01-01 00:0	2022-12-22 16:3	clientTransferPr
nvidia.com.ph				dns3.idp365.net|dns1.idp365.net|dns2.idp365.net|						
nvidia.co.ve	NIC-VE		whois.nic.ve	dns2.idp365.net|	23.10.2015 11:1	13.03.2020 11:2	31.05.2023	2015-10-23 11:1	2020-03-13 11:2	2023-05-31 00:00:00 UTC	
nvidia.co.id	PT. Web Comme	support@mereki	whois.pandi.or.id	dns1.idp365.net|	20/01/2016 10:0	09/01/2022 16:0	20/01/2023 00:0	2016-01-20 10:0	2022-01-09 16:0	2023-01-20 00:0	clientUpdatePro
nvidia.co.nz	Safenames Ltd	hostmaster@saf	whois.srs.net.nz	dns1.idp365.net|	2010-01-06T00:	2021-12-29T13:34:17+13:00		2010-01-06 00:0	2021-12-29 00:00:00 UTC		200 Active
nvidia.gg			whois.dominio.gg								
nvidia-uk-ltd.com	Wild West Doma	abuse@wildwes	whois.wildwestdomains.com	NS1.BDM.MICR	2022-04-15T03:	2022-04-15T03:	2023-04-15T03:	2022-04-15 03:1	2022-04-15 03:1	2023-04-15 03:1	clientTransferPr
nvidia.my.id	PT Cloud Hostin	care@idcloudho	whois.pandi.or.id	amber.ns.cloudfl	05/04/2022 6:09	03/08/2022 8:09	05/04/2023 0:09	2022-04-05 06:0	2022-08-03 08:0	2023-04-05 00:0	ok
nvidia.id	PT. Web Comme	support@mereki	whois.pandi.or.id	dns1.idp365.net|	30/09/2014 10:0	06/09/2021 9:09	30/09/2022 00:0	2014-09-30 10:0	2021-09-06 09:0	2022-09-30 00:0	clientUpdatePro

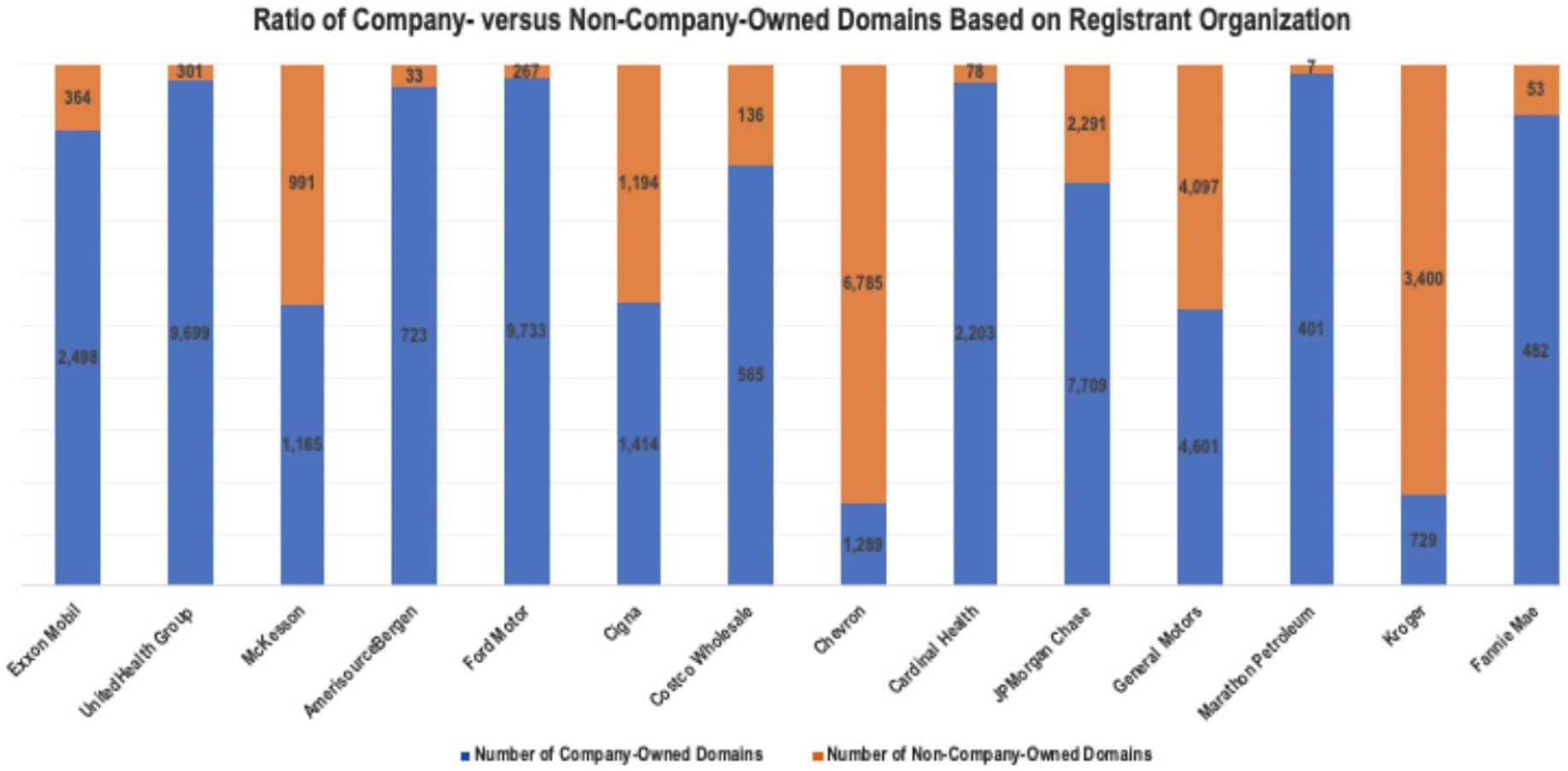
建議: 善加利用 Whois 歷史數據和域名DNS數據
進而釐清資產關聯性與數位足跡

nvidia-omniverse	100	
nvidia-381.8x8.u	100	
nvidiaglahblog.b	100	
nvidia-geforce-d	100	
nvidia.companys	100	
nvidia-shadowpla	100	
nvidia-book-scar	100	
nvidia.zoom.us	100	
nvidia.ibl.educati	100	
nvidia-api.torchli	100	
nvidia.agichi.co	81.25	Malware
nvi		
nvi		
nvi		
nvidia-experienc	100	
nvidia-highlights-	100	
nvidia-lic-dev.ah	100	
nvidiaomniverse.	100	
nvidia.fot.ma	100	
nvidia123.firebas	100	
nvidia5.blogspot.	100	
nvidiamei.y088.c	100	
nvidia.nvidia-shi	100	

http://nvidia.agichi.com/

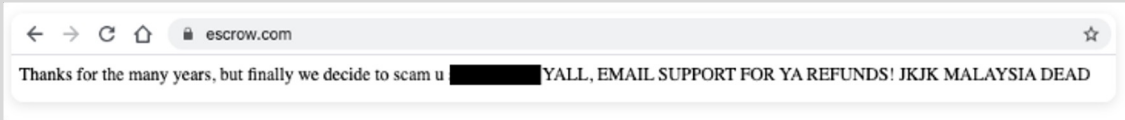


域名仿冒 / BEC

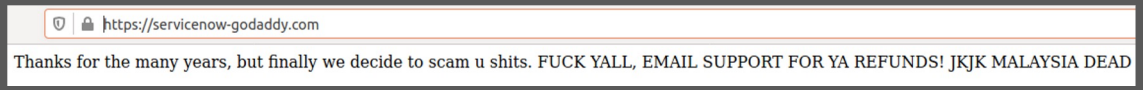

Ratio of Company- versus Non-Company-Owned Domains Based on Registrant Organization
364
2,498
301
9,699
991
1,165
33
723
267
9,733
1,194
1,414
136
565
6,785
1,289
78
2,203
2,291
7,709
4,097
4,601
7
401
3,400
729
53
482
Exxon Mobil
UnitedHealth Group
McKesson
AmerisourceBergen
Ford Motor
Cigna
Costco Wholesale
Chevron
Cardinal Health
JPMorgan Chase
General Motors
Marathon Petroleum
Kroger
Fannie Mae
Number of Company-Owned Domains
Number of Non-Company-Owned Domains

E-ASM : Domain Name Registrar

“Phish of GoDaddy Employee Jeopardized Escrow.com, Among Others”



The profanity-laced message left behind by whoever briefly hijacked the DNS records for escrow.com. Image: Escrow.com



The message at servicenow-godaddy[.]com was identical to the one displayed by escrow.com while the site’s DNS records were hacked.

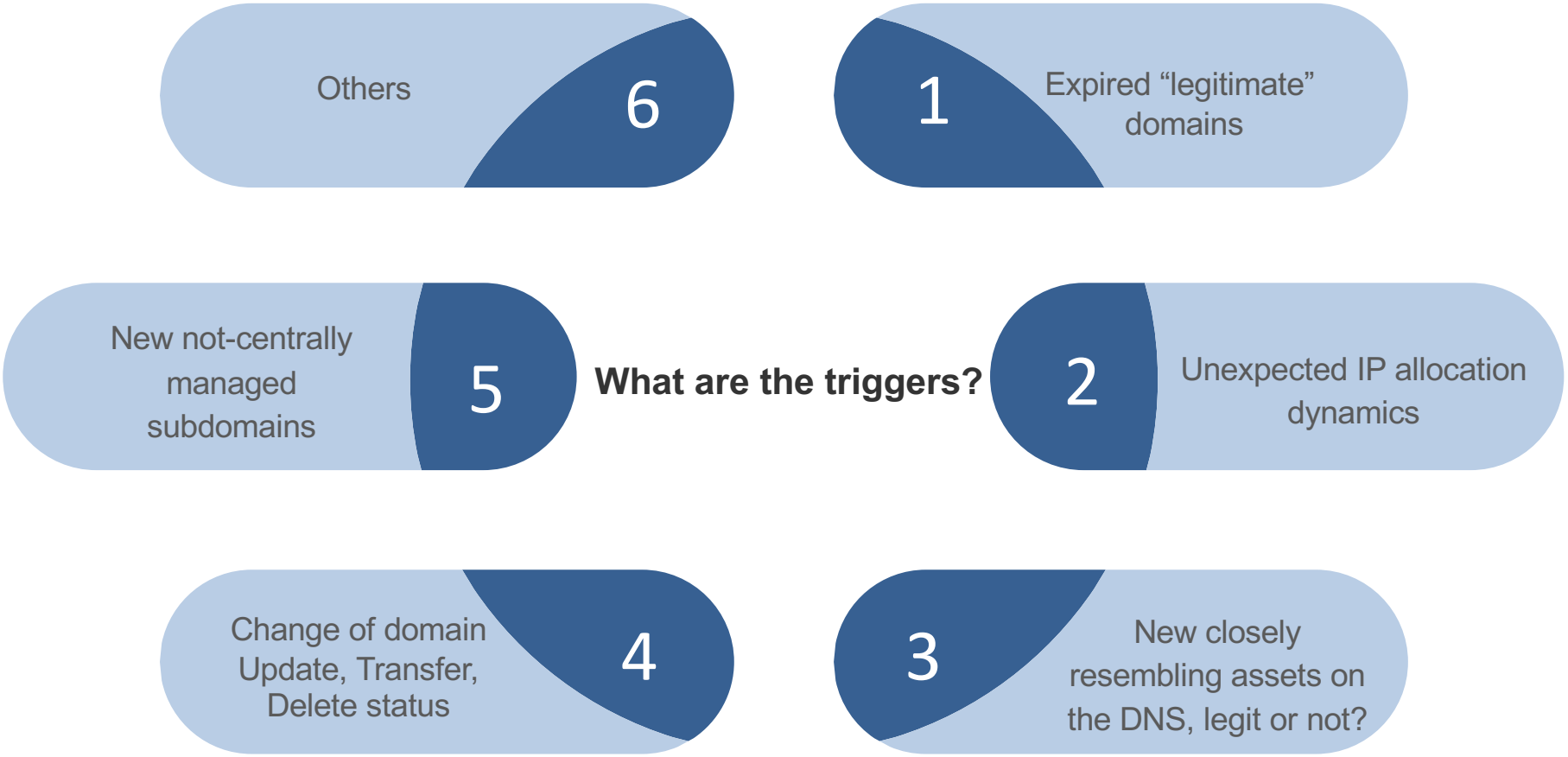
Source: KrebsonSecurity.com

.brand 品牌頂級域 ？

https://tw.canon

https://tw.sharp

ASM – Defensive Approach



總結

- **Crossing Chasm**
  - 理解 ASM 概念不難, 而實際執行是對企業管理模式與預算的挑戰, 存在巨大的落差!
  - ASM 週期(監測 ➡ 發現 ➡ 處理) 若沒有完整網路核心數據是做不到的!
- **Paradigm Shift**
  - 從 “Asset” Centric 到 ”Security” Centric
  - 並非減少ASM攻擊面就好, 而是企業成長時, 每個可視的網路資產都經 ASM 機制進行管理
- **N到 N+2**
  - 數位資產(數位品牌)保護延伸至相關供應商安全能力(認證資格)和信譽

做好ASM管理，
從掌握網路核心數據做起!

WhoisXMLAPI : Internet Infrastructure Data

	Product	Frequency / updates
	WHOIS Database Feed	Real-time / Daily, with historical data
	Subdomains Database Feed	Weekly
	Website Contacts & Categorization Database	Daily
	DNS Database Feed Download	Weekly
	IP Netblocks (IPv4 + IPv6)	Daily
	IP Geolocation Database	Weekly, unlimited sites
	Typosquatting Data Feed (standard + enriched)	Daily
	Disposable Email Domains Feed	Daily

WhoisXMLAPI : Data Integrations

splunk>

MALTEGO

Amass
OWASP®

Radar

servicenow

WHOISAT™

and many others...

超過 50,000 家頂尖網路安全公司、知名IT製造業者與跨國金融業者
採用WhoisXMLAPI數據服務

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

www.whoisxmlapi.com

chiao@whoisxmlapi.com

www.chingchiao.com