


So Long (Go)Daddy | Tracking BlackTech Infrastructure

 cyberandramen.net/2022/09/24/so-long-godaddy-tracking-blacktech-infrastructure/

September 24, 2022

Summary

BlackTech has built a reputation relying on (much to the delight of defenders) tech-themed domains and predictable registration patterns. Recent reporting linking malicious domains to the actor suggests these patterns may be fading, at least for the time being signifying a departure from the previous infrastructure configuration.

Items to Note

- Failure to redact email addresses within WHOIS records (mitsumori.gb@gmail[.]com, wufi2011@gmail[.]com, siraiya128@gmail[.]com, senotice@gmail[.]com) leads to dozens more domains likely linked to the actor(s).
- BlackTech prefers dynamic DNS services, with most of the domains' registrars being GoDaddy, paired with domaincontrol[.]com name servers (NS).
- Domain naming conventions centered around technology/target (recent intrusion reporting shows this pattern may change).

Background

BlackTech, a.k.a. Huapi, Temp.Overboard, Circuit Panda, Radio Panda is a cyber espionage actor routinely associated but never publicly attributed to Chinese security services. Primary targets of the actor include the technology, financial and government sectors in Taiwan, Hong Kong, Japan, and recently the U.S.

Please refer to the excellent reporting by JPCert, NTT, TrendMicro, and PWC's @cyberoverdrive and @malworms.

Infrastructure New & Old

The data captured in this post uses multiple vendor reports and VirusTotal and RiskIQ to gather passive DNS data. One hundred thirty (130) domains linked to BlackTech were identified and added to a CSV file along with first-seen dates, registrant and registrar information, and name server information.

1	domain	first_seen	registrar	registrant	ns
2	ericspan.sll443.org	6/2012	Name.com	Domain Protections Services	name.com
3	windows.ssl443.org	6/2012	PDR Ltd	N/A	changeip.com
4	itaiwans.com	1/2013	GMO, Onamae	N/A	changeip.com
5	goodnewspaper.f3322.org	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
6	goodnewspaper.3322.org	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A

7	goodnewspaper.gicp.net	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
8	xinxin20080628.gicp.net	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
9	xinxin20080628.3322.org	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
10	uyghur.sov.tw	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
11	www.uyghur.mrface.com	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
12	uyghri.mrface.com	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
13	uyghur.51vip.biz	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
14	uyghur1.webhop.net	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
15	uygur.eicp.net	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
16	uyghur.epac.to	9/2013	Shanghai Best	REDACTED FOR PRIVACY	N/A
17	butterfly.xxuz.com	8/2014	PDR Ltd	changeip operations	changeip.com
18	truecoco.rebatesrule.net	8/2014	PDR Ltd	changeip operations	changeip.com
19	web2008.rutentw.com	12/2015	GoDaddy	Domains By Proxy	domaincontrol.com
20	k3ad01.rutentw.com	12/2015	GoDaddy	Domains By Proxy	domaincontrol.com
21	twncisi.ignorelist.com	3/2016	Porkbun	Socketfire, Inc	afraid.com
22	fatgirls.fatdiary.org	9/2016	GoDaddy	Jidea	afraid.com
23	twcertcc.jumpingcrab.com	8/2016	Porkbun	Private By Design, LLC	afraid.com
24	update.forticlient.tw	2/2017	Name.com	Domain Protections Services	name.com
25	lang.suroot.com	2/2017	N/A	N/A	namebrightdns.com
26	gstrap.jkub.com	3/2017	PDR Ltd	N/A	changeip.com
27	sso.forticlient.tw	4/2017	Name.com	Domain Protections Services	name.com
28	shopping.kddi-cloud.com	4/2017	GoDaddy	Domains By Proxy	domaincontrol.com
29	okinawas.ssl443.org	7/2017	PDR Ltd	N/A	changeip.com
30	kyguxs.dnset.com	7/2017	PDR Ltd	Overtures Infotech	changeip.com
31	langlang.dnset.com	7/2017	PDR Ltd	Overtures Infotech	changeip.com
32	lookatinfo.dnset.com	7/2017	PDR Ltd	Overtures Infotech	changeip.com
33	savecars.dnset.com	7/2017	PDR Ltd	Overtures Infotech	changeip.com
34	sslmaker.ssl443.org	7/2017	PDR Ltd	N/A	changeip.com
35	fortigatecloud.com	9/2017	GoDaddy	Domains By Proxy	domaincontrol.com
36	cybermon.fortigatecloud.com	9/2017	GoDaddy	Domains By Proxy	domaincontrol.com
37	comodoca.fortigatecloud.com	9/2017	GoDaddy	Domains By Proxy	domaincontrol.com
38	agent.fortigatecloud.com	9/2017	GoDaddy	Domains By Proxy	domaincontrol.com
39	website.fortigatecloud.com	9/2017	GoDaddy	Domains By Proxy	domaincontrol.com
40	ntp.ukrootns1.com	10/2017	Shanghai Meic	REDACTED FOR PRIVACY	ezdnscenter.com
41	jpgcerts.jpgcertinfo.com	1/2018	Onamae, Disc	siraiya128@gmail.com	value-domain.com
42	dev.panasocin.com	1/2018	Name.com	Domain Protections Services	name.com
43	labs.panasocin.com	1/2018	GoDaddy	Domains By Proxy	domaincontrol.com
44	office.panasocin.com	1/2018	GoDaddy	Domains By Proxy	domaincontrol.com
45	update.panasocin.com	1/2018	GoDaddy	Domains By Proxy	domaincontrol.com
46	jpgcert.ignorelist.com	1/2018	Porkbun	Socketfire, Inc	afraid.com
47	adobeupdate.serveusers.com	3/2018	PDR Ltd	changeip operations	changeip.com
48	em.totalpople.info	4/2018	GMO, Onamae	Whois Privacy Prot	N/A
49	woc.yasonbin.info	4/2018	GMO, Onamae	Whois Privacy Prot	value-domain.com
50	appstore.androiddatacenter.com	6/2018	Name.com	Domain Protections Services	name.com
51	webs.shopcart.otzo.com	9/2018	PDR Ltd	changeip operations	changeip.org
52	update.helps.zyns.com	10/2018	PDR Ltd	changeip operations	changeip.com
53	centosupdates.online	11/2018	GoDaddy	Domains By Proxy	domaincontrol.com
54	azure.kddi-cloud.com	11/2018	Name.com	Domain Protections Services	name.com
55	webssl.kddi-cloud.com	11/2018	Name.com	Domain Protections Services	name.com
56	app.dynamicrosoft.com	2/2019	GoDaddy	Domains By Proxy	domaincontrol.com
57	www.vmware.com.dynamicrosoft.com	2/2019	GoDaddy	Domains By Proxy	domaincontrol.com
58	home.dynamicrosoft.com	2/2019	GoDaddy	Domains By Proxy	domaincontrol.com
59	home.nttatcloud.com	2/2019	Name.com	Domain Protections Services	name.com
60	microsoft.com.appstore.dynamicdns.co	2/2019	eNom LLC	N/A	changeip.com
61	ap21.gckerda.com	3/2019	GoDaddy	Domains By Proxy	domaincontrol.com
62	gckerda.com	3/2019	GoDaddy	Domains By Proxy	domaincontrol.com
63	www.google.com.dns-report.com	4/2019	PDR Ltd	changeip operations	changeip.com
64	cartview.viamissoftware.com	5/2019	eNom LLC	N/A	afraid.com
65	ssl.forticlient.tw	7/2019	PDR Ltd	N/A	changeip.com
66	kyu.forticlient.tw	7/2019	GoDaddy	Domains By Proxy	domaincontrol.com

Figure 1: Snippet of CSV

CSV files allow for identifying possible campaign time-lining and visualizing trends or patterns in BlackTech infrastructure tactics, techniques, and procedures (TTPs). Reusing domains and overlapping infrastructure across different intrusion sets have become a calling card for the actor(s).

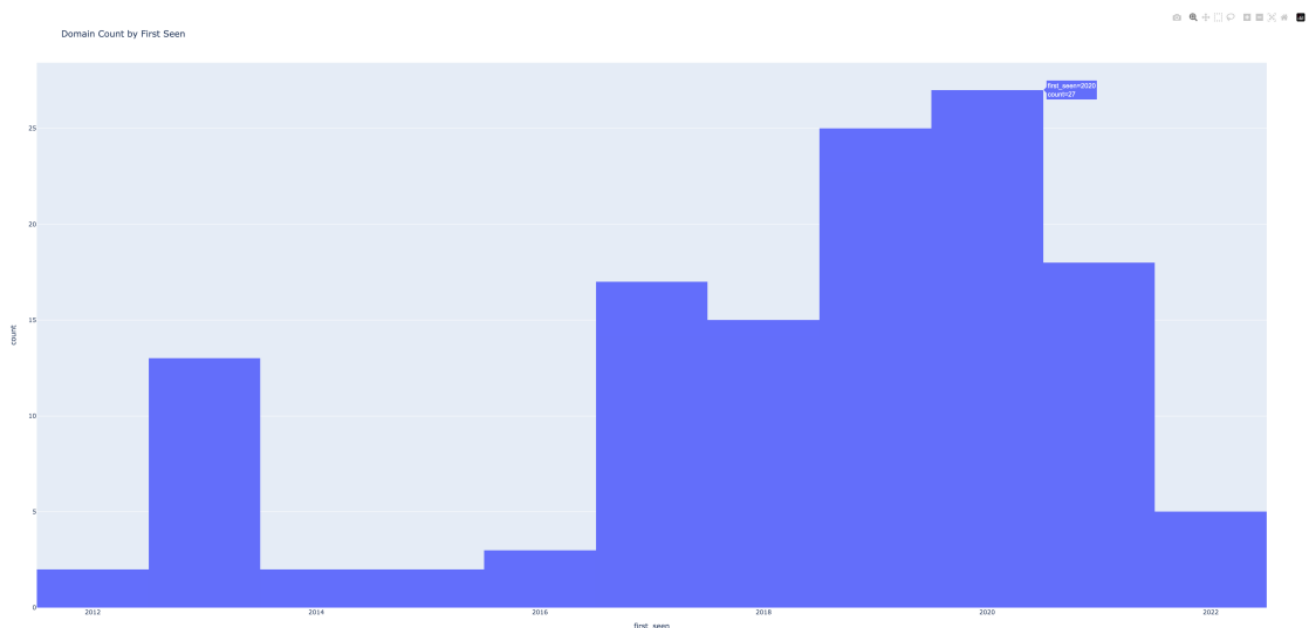


Figure 2: Domains by year

The lone spike seen in Figure 1 in 2013 is in large part due to the “Four-Element Sword Engagement.”

Constituting nearly a third of the domains registered, GoDaddy and domaincontrol[.]com NS have provided defenders with clues to out related infrastructure before put in use.

As seen in the below scatter plot, PDR Ltd. and Vitalwerks Internet Solutions, LLC represents the majority of registrars linked to BlackTech recently.

This activity consists of registrar changes in addition to name server information, as seen in Figure 4.

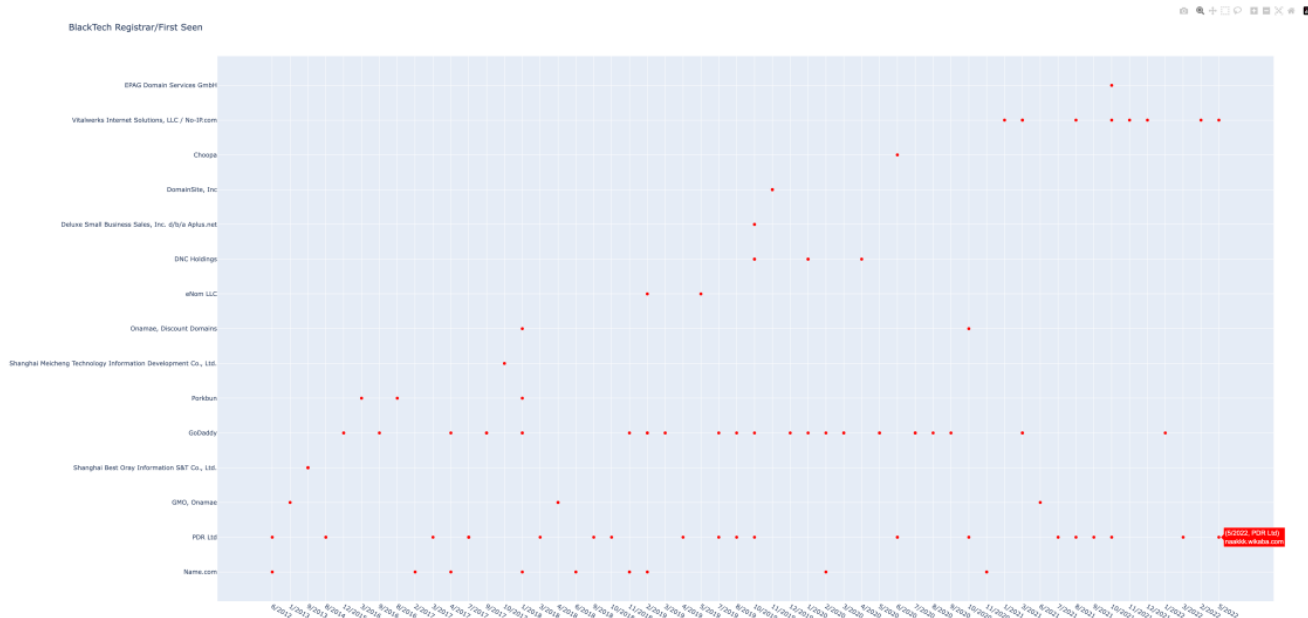


Figure 3: Scatter plot of registrar use by month/year

Previously, defenders may have enjoyed success querying for tech-themed dynamic DNS domains registered to GoDaddy with domaincontrol NS. While small wins in the above hunting category may prove fruitful, updated infrastructure configurations should be considered and watched closely.

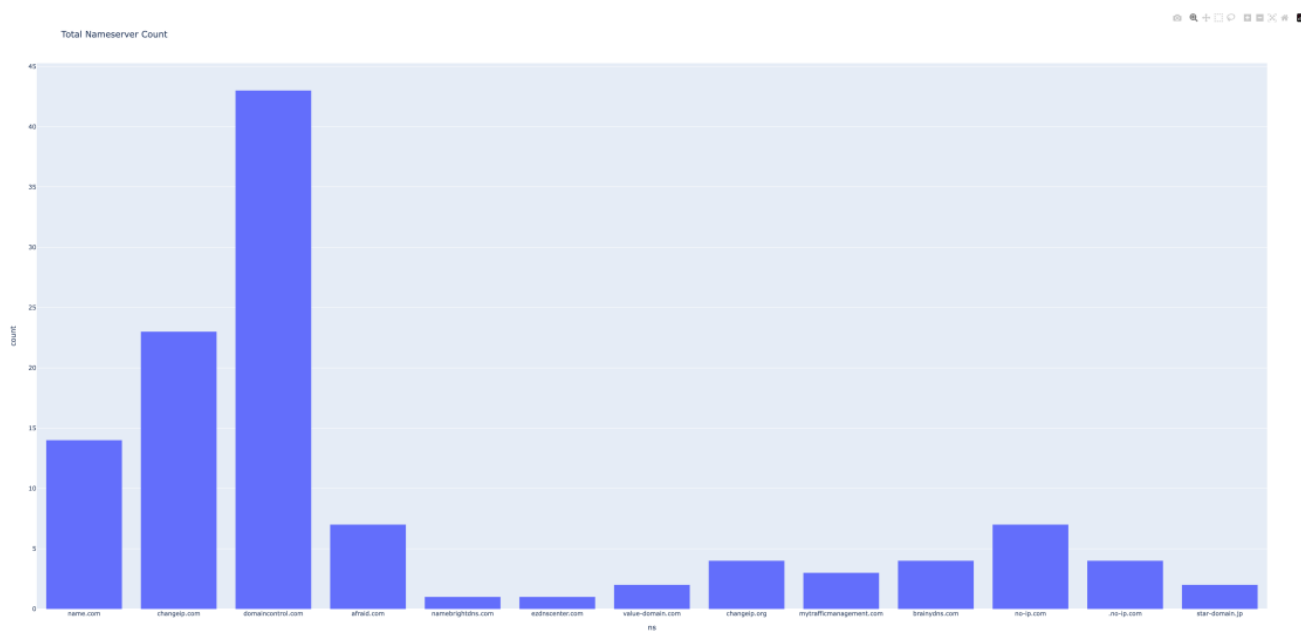


Figure 4: Name server count

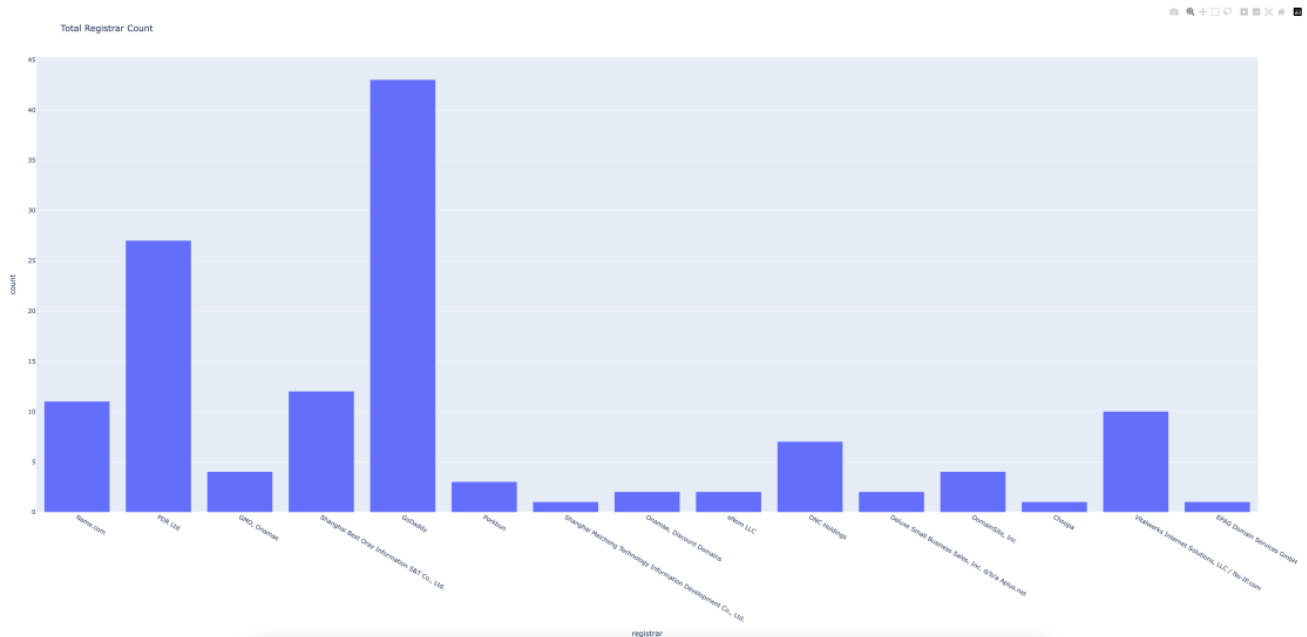


Figure 5: Registrar count

Stepping back to look at the above data, three assumptions arise (I will leave the true analysis to the experts):

- The change in infrastructure is only temporary, and a return to normal patterns will return.
- The above behavior indicates a group that has had infrastructure burned by security vendors and researchers on social media.
- BlackTech campaigns call for different hosting configurations, explaining the change.

Unfortunately, when it comes to the inner workings of not only BlackTech but many APT groups, few defenders have inside knowledge of day-to-day operations.

Only continued analysis with multiple colored Excel spreadsheets to track changes will inch Blue Teamers closer to understanding one of the above assumptions.

Conclusion

While these configuration changes may not represent breaking news, identifying adversary infrastructure before malicious activity ensues is very important for defenders.

Like puzzle pieces, registrant names and name servers alone may not provide a pretty picture, but when paired with consistent naming themes and other registration information, a clearer picture of an adversary emerges.