GDPR: harmless after all?

Europe's GDPR, Whois shakeup was supposed to trigger spam tsunami – so, er, where is it?

There may be many reasons f
vaunted value of Whois data h
because the genuinely nefario
name, fake address, fake telephone numbers.

Domain Registrations Have Fallen Slightly Since May

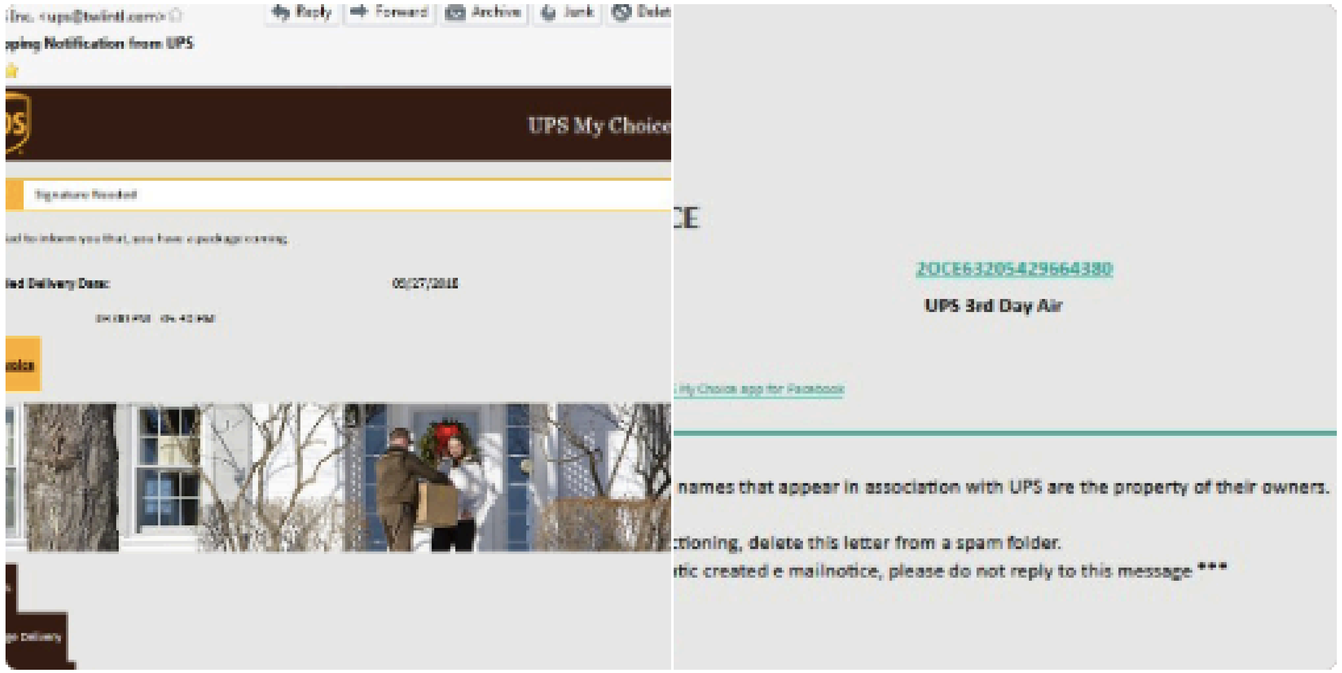
Average daily new domain registrations have actually fallen slightly since May 25, 2018. For the month leading to the enactment of the GDPR, Recorded Future collected an average of more than 223,500 new domain registrations each day. From May 26 to July 2, 2018, the average number of new domain registrations was 213,300 — a slight drop off of 10,000 new domain registrations per day.

GDPR: harmless after all?

#hancitor

GarWarner @GarWarner · 15h

Today's #Hancitor #Malware #Spam imitates a UPS invoice. It tries to get you to click your "Tracking number" in my case, that goes to "genesisofdenver [dot] com" to complete the infection



Domain: genesisofdenver.com

IP: 47.254.198.10

Registrant email: 8FC0

Domain	Registrar
carvanacharlotte.com	GoDaddy
carvanachicago.com	GoDaddy
carmaxoflouisville.com	GoDaddy
louisvillecarmax.com	GoDaddy
louisvillerides.com	GoDaddy
louisvilleride.com	GoDaddy
carmaxlouisville.com	GoDaddy
ridesharelouisville.com	GoDaddy
kccmanufacturing.com	GoDaddy
oxmoorsucks.com	GoDaddy
oxmoorbuyscars.com	GoDaddy
…	GoDaddy
oxmoorcars.com	GoDaddy
kyshieldinsurance.com	GoDaddy
…	GoDaddy

- 58 domains total
- on 28 different IPs
- many on massive vhosting
- many used by hancitor
- All of them maybe?

Registrant email: 8FC0

Domain	Registrar
carvanacharlotte.com	GoDaddy
carvanachicago.com	GoDaddy
carmaxoflouisville.com	GoDaddy
louisvillecarmax.com	GoDaddy
louisvillerides.com	GoDaddy
louisvilleride.com	GoDaddy
carmaxlouisville.com	GoDaddy
ridesharelouisville.com	GoDaddy
kccmanufacturing.com	GoDaddy
oxmoorsucks.com	GoDaddy
oxmoorbuyscars.com	GoDaddy
…	GoDaddy
oxmoorcars.com	GoDaddy
kyshieldinsurance.com	GoDaddy
…	GoDaddy

- new hancitor campaign
- domains from the same list
- DBL marks 'em all as malware domains…

Registrant email: 8FC0

Domain	Registrar
carvanacharlotte.com	GoDaddy
carvanachicago.com	GoDaddy
carmaxoflouisville.com	GoDaddy
louisvillecarmax.com	GoDaddy
louisvillerides.com	GoDaddy
louisvilleride.com	GoDaddy
carmaxlouisville.com	GoDaddy
ridesharelouisville.com	GoDaddy
kccmanufacturing.com	GoDaddy
oxmoorsucks.com	GoDaddy
oxmoorbuyscars.com	GoDaddy
…	GoDaddy
oxmoorcars.com	GoDaddy
kyshieldinsurance.com	GoDaddy
…	GoDaddy

- new campaign picks domain from the same list
- probably campaign goes nowhere…

#hancitor

GarWarner
@GarWarner

Following

Today's #Hancitor #Malware #Spam is imitating @DHLUS. My copy includes malicious links at "dcbadfoodlawyer (dot) com"

…so they move to a different
atch of domains…

Domain: dcbadfoodlawyer.com

Domain	Registrar	Registrant email
dcbadfoodlawyer.com	GoDaddy	D1D7

Registrant email: D1D7

Domain	Registrar	Registrant email
dcbadfoodlawyer.com	GoDaddy	D1D7
laleyenespanol.net	GoDaddy	D1D7
laleyenespanol.info	GoDaddy	D1D7
havanacounsel.com	GoDaddy	D1D7
pitchmiami.com	GoDaddy	D1D7
pitchthevalley.com	GoDaddy	D1D7
pitchchicago.com	GoDaddy	D1D7
pitchaustin.com	GoDaddy	D1D7
milliondollarlawsuit.co	GoDaddy	D1D7
visithavana.co	GoDaddy	D1D7
puertoricanlawblog.com	GoDaddy	D1D7
floridafinancialfraudlawyer.com	GoDaddy	D1D7
redteamlawyers.com	GoDaddy	D1D7
sarelsonlawfirm.com	GoDaddy	D1D7
…	GoDaddy	D1D7

Registrant email: D1D7

Domain	Registrar	Registrant email
dcbadfoodlawyer.com	GoDaddy	D1D7
laleyenespanol.net	GoDaddy	D1D7
laleyenespanol.info	GoDaddy	D1D7
havanacounsel.com	GoDaddy	D1D7
pitchmiami.com	GoDaddy	D1D7
pitchthevalley.com	GoDaddy	D1D7
pitchchicago.com	GoDaddy	D1D7
pitchaustin.com	GoDaddy	D1D7
milliondollarlawsuit.co	GoDaddy	D1D7
visithavana.co	GoDaddy	D1D7
puertoricanlawblog.com	GoDaddy	D1D7
floridafinancialfraudlawyer.com	GoDaddy	D1D7
redteamlawyers.com	GoDaddy	D1D7
sarelsonlawfirm.com	GoDaddy	D1D7
…	GoDaddy	D1D7

Registrant email: D1D7

Domain	Registrar	Registrant email
dcbadfoodlawyer.com	GoDaddy	D1D7
laleyenespanol.net	GoDaddy	D1D7
laleyenespanol.info	GoDaddy	D1D7
havanacounsel.com	GoDaddy	D1D7
pitchmiami.com	GoDaddy	D1D7
pitchthevalley.com	GoDaddy	D1D7
pitchchicago.com	GoDaddy	D1D7
pitchaustin.com	GoDaddy	D1D7
milliondollarlawsuit.co	GoDaddy	D1D7
visithavana.co	GoDaddy	D1D7
puertoricanlawblog.com	GoDaddy	D1D7
floridafinancialfraudlawyer.com	GoDaddy	D1D7
redteamlawyers.com	GoDaddy	D1D7
sarelsonlawfirm.com	GoDaddy	D1D7
…	GoDaddy	D1D7

Registrant email: D1D7

Domain	Registrar	Registrant email
dcbadfoodlawyer.com	GoDaddy	D1D7
laleyenespanol.net	GoDaddy	D1D7
laleyenespanol.info	GoDaddy	D1D7
havanacounsel.com	GoDaddy	D1D7
pitchmiami.com	GoDaddy	D1D7
pitchthevalley.com	GoDaddy	D1D7
pitchchicago.com	GoDaddy	D1D7
pitchaustin.com	GoDaddy	D1D7
milliondollarlawsuit.co	GoDaddy	D1D7
visithavana.co	GoDaddy	D1D7
puertoricanlawblog.com	GoDaddy	D1D7
floridafinancialfraudlawyer.com	GoDaddy	D1D7
redteamlawyers.com	GoDaddy	D1D7
sarelsonlawfirm.com	GoDaddy	D1D7
…	GoDaddy	D1D7

Rinse & Repeat

Operational steps forward

Investigation doesn't need cleartext

Correlation -not identification- is step 1

- → 8FC0: XXXXX@msn.com
- → D1D7: YYYYY@yahoo.com

Without correlating first, identification is worthless (in most cases)