Terri Agnew:Welcome to the GNSO Webinar on ICANN Domain Abuse Reporting Tool (DART), with presenter Dave Piscitello on Wednesday, 14 June 2017 at 20:00 UTC for 60 mins.

Terri Agnew:DART is a platform for studying domain name registration and reporting abuse behavior across top-level domain (TLD) registries and registrars. DART was designed to provide the ICANN community with a neutral, unbiased, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed. The system collects a very large body of registration data and complements this with a large set of high-confidence reputation (threat) data feeds. The data collected by the DART system can serve as a platform for studying daily or historical registration or abuse activities and for reporting activity. The overarching purpose of DART is to give the ICANN community reliable, unbiased data that can be used to make informed consensus policy decisions.

Matthias Pfeifer .berlin:good evening all

Martin Silva:Hi all

Maxim Alzoba (FAITID):Hello All

Matthias Pfeifer .berlin:question: did the system looks for all TLDs or just the new gTDLs in the source data?

Maxim Alzoba (FAITID):Question:the current ICANN stance looks like SPAM is separated from security threats. Is it going to be changed? /Question

Michele Neylon:It's all gTLDs

Michele Neylon:not just new ones

Matthias Pfeifer .berlin:well..so this project can do the spec11 job for us

Maxim Alzoba (FAITID):@Matthias, most probably for ICANN Compliance

Matthias Pfeifer .berlin:i see ;)

Maxim Alzoba (FAITID):are ccTLD tracking is a part of the project?

Maxim Alzoba (FAITID):<QUESTION>are ccTLD tracking is a part of the project?</QUESTION>

Donna Austin, Neustar:Who is the 'operational security community'?

Maxim Alzoba (FAITID):security operation experts?

Donna Austin, Neustar:@Maxim, even that is really broad.

Keith Drazek:Qustion: On Whois data, how does the DART deal with or treat Privacy/Proxy services?

Maxim Alzoba (FAITID):<QUESTION> is it possible to publish URL for this slidedeck ? </QUESTION>

Maxim Alzoba (FAITID):<QUESTION>IS it possible to see , which particular lists used for DART? Not very Registry is happy with all of them</QUESTION>

Nathalie Peregrine:@ Maxim, the slide deck will be published on the GNSO Master calendar here: https://urldefense.proofpoint.com/v2/url?u=https-3A__gnso.icann.org_en_group-2Dactivities_calendar-23jun&d=DwICaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=DRa2dXAvSFpCIgmkXhFzL7ar9Qfqa0AIgn-H4xR2EBk&m=THn0hr5OZfacwoz-IxjCvlzZavviNIOiMr5CFfFP4Jo&s=_L4bXcdE0KlSf9l2Tnas-VaiGk2xs14qcxgE86KPwkk&e=

Matthias Pfeifer .berlin:<questions>it is possible to see threads per TLD list with the used data sources?</question>

Maxim Alzoba (FAITID):<QUESTION> Is it possible to see particular URLs to proofs, provided by lists? without it DART will be useless for Registries</QUESTION>

James Bladel:Question: Is this all rolled up to the gTLD second-level domain? For example, if several compromised sites are at Wordpress.com or Blogger.com, would they count as a single instance against that domain (and regisrar/registry)?

Matthias Pfeifer .berlin:@maxim most of the data in the feeds has a very short "lifetime" :/

Matthias Pfeifer .berlin:a serious issue when we try to do some documentation of threats

Maxim Alzoba (FAITID):@Matthias, we need it in a day or so, not as a history . Blind trust leads to dark spaces

Matthias Pfeifer .berlin::)
Maxim Alzoba (FAITID):<QUESTION> it is going to be not much time for answers. Could we expect that ICANN staff sends answers chat questions to RrSG and RySG ExComs?</QUESTION>
James Bladel:Probably brand TLDs with little to no use. Consider only reporting on non-zero TLDs
Matthias Pfeifer .berlin:so long we can not see TLDs in scoring we cannot make any conclusion..related to whois accuracy etc.
Maxim Alzoba (FAITID):if a brand decides to send Ads. to it's clients - it could expect to be top rated :)
Matthias Pfeifer .berlin:such a brand will probably use another domain ;)
James Bladel:So ICANN is snowshoeing WHOIS queries to circumvent rate limits that protect harvesting?
Michele Neylon:James - yes
Maxim Alzoba (FAITID):removing limits for security experts will lead to lots of new "security experts", who are more interested in whois unlimited access ... it is going to be gamed
James Bladel:Rate limiting is a safeguard, not a problem to be solved.
Matthias Pfeifer .berlin:<question> why icann/DART will not publish tld/threat relation data?</question>
Maxim Alzoba (FAITID):<QUESTION> IS it planned to actually consult with Registrars and Registries - which kinds of data would be useful for them?<QUESTION>
James Bladel:Question: Your description of use of WHOIS data appears to violate our (GoDaddy's) Terms of Use. Did you obtain explicit permisson from registrars to harvest whois data for this project?
Benny Samuelsen / Nordreg AB:<question> How is this collecting of data treathed and handled with regards to the upcoming GDRP provisions ?</question>
Keith Drazek:So no ccTLDs?
Matthias Pfeifer .berlin:thx Dave
Maxim Alzoba (FAITID):most ccTLDs have some reluctance to giving out zone files
Michele Neylon:In our experience a lot of the dodgy domains are paid for with stolen cards or hacked paypal credentials
Maxim Alzoba (FAITID):if we are unable to filter out spam - the tool is going to be not very useful for Spec 11 for ROs
Maxim Alzoba (FAITID):when blocklist blocklists us for an attemt to contact them - it is a bad sign
Michele Neylon:We use it on our inbound mail - it blocks 90+ % of inbound SMTP connections
Matthias Pfeifer .berlin:please close that question
Matthias Pfeifer .berlin:it has already been answerd
Maxim Alzoba (FAITID):suggestion : please use Public suffix list
Maxim Alzoba (FAITID):it is a well known source of info for 3rd levels e.t.c.
Matthias Pfeifer .berlin:thx maxim!
Matthias Pfeifer .berlin:i would like to see a tld/threat relation
Matthias Pfeifer .berlin:so threats is not a matter of policy and price?..for example?
Keith Drazek:The ability to identify and track domain-hopping (the transfer of abusive behavior) from one TLD to anther would be very interesting. But that would only be meaningful if ccTLDs were included.
Matthias Pfeifer .berlin:*threats are
Matthias Pfeifer .berlin:no, sorry
Matthias Pfeifer .berlin:ok, thank you
James Bladel:I'm confused, you said you were working to "resolve the problem" of rate limits.
Kristina Rosette (Amazon Registry):And, btw, if memory serves, new gTLD registry operators were given an extra point for implementing Whois rate limiting.
Graeme Bunton:I would like to be in on that too.
Ben Butler:I am and I would be happy to have that conversation

Maxim Alzoba (FAITID):it will increase number of security experts instantly
Ronald Schwaerzler - .wien:sorry for joining late
Graeme Bunton:(From Tucows, FYI)
James Bladel:Let's not engage in abusive tactics in the quest to root out Abuse. :)
Michele Neylon:lo
Michele Neylon:lol
Maxim Alzoba (FAITID):GDPR?
Michele Neylon:GDPR
James Bladel:But just grabbing Registrar of Record should be ok, if not Contact objects
Ben Butler:Correct - The name servers and registrar of record are not PII, and should not be in scope for GDPR
Benny Samuelsen / Nordreg AB:Ok so no personal data collected?
Graeme Bunton:Pretty sure whois data will fall under GDRP, see: https://urldefense.proofpoint.com/v2/url?u=https-3A__www.whitecase.com_publications_article_chapter-2D5-2Dkey-2Ddefinitions-2Dunlocking-2Deu-2Dgeneral-2Ddata-2Dprotection-2Dregulation&d=DwICaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=DRa2dXAvSFpCIgmkXhFzL7ar9Qfqa0AIgn-H4xR2EBk&m=THn0hr5OZfacwoz-IxjCvlzZavviNIOiMr5CFfFP4Jo&s=vVzDDBp3W6_w6VmRiT2ymbiMbnDsf19CHcO6KQL14xM&e=
Michele Neylon:Graeme - yes, but not the bits they're using
Benny Samuelsen / Nordreg AB:Ok that answer my question
Benny Samuelsen / Nordreg AB:thanks
Michele Neylon:it doesn't use the registrant details
Maxim Alzoba (FAITID):in NL - IP address might be seen as a personal data :)
Michele Neylon:registrar + nameservers and not much else
Michele Neylon:Maxim - the IP address of a nameserver isn't PII
Michele Neylon:my DSL / home IP is
Maxim Alzoba (FAITID):if I am stupid enough to install it in home and to add geo tag :)
James Bladel:And if you're hosting DNS records from your home machine? :
Michele Neylon:James - well you're an idiot in that case :)
Maxim Alzoba (FAITID):or me
Michele Neylon:cos the amount of junk you'd get would be insane
James Bladel:Thanks, all.  Good session.
Matthias Pfeifer .berlin:thank you so far :)
Frank Michlick:Thank you
Michele Neylon:ciao
Maxim Alzoba (FAITID):bye all
Eric Rokobauer:thank you!
Sean Baseri - Neustar:thanks all