

Exposing the "Patriot Front" Online Hate Group -An OSINT Analysis

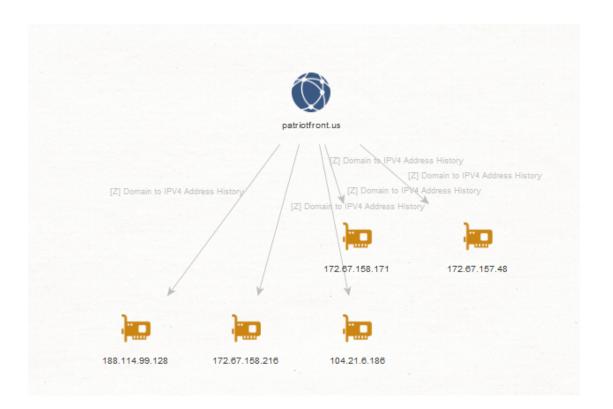
						patriotfront.us	
04-29 04:48:19 UTC 2021	To Histori	Historical WHOIS Records [Whois earl WHOIS Records [WhoisXML] 2021-01-28 21:58:54 UTC 2	XML] Te Historical WHOIS R To Historical WHO	I WHOIS Records [WhoisXML] To Historical WHOIS Re cords [WhoisXML] IS Records [WhoisXML]		To Historical WHOIS R WhoisXML] IS Records (WhoisXINE Historical WH	To Histor
*	-	-	-	-	-	-	:-
patriotfront.us	patriotfront.us	patriotfront.us	patriotfront.us	patriotfront.us	patriotfront.us	patriotfront.us	patriotfr
gistrant Emäil Address_ Regist		Registrant Email Address	evense WHOIs Search/Whois	angeremain Address	To Domains and IP Addres	Registrant Email Address Registr	
		pa	triotfront@protonmail.com	1			

In this brief analysis Dancho Danchev a DNS Threat Researcher at WhoisXML API will provide a brief OSINT analysis on the Internet-connected infrastructure of the recently busted online hate group known as "Patriot Front" and will offer additional insights into its Internet-connected infrastructure for the purpose of assisting U.S Law Enforcement on its way to track down and monitor and eventually prosecute members of the "Patriot Front" online hate group.

Sample URLs known to have been involved in the campaign:

hxxp://patriotfront.us hxxp://bloodandsoil.us hxxp://gigabitplexus.com





Sample personal email address accounts known to have been involved in the campaign:

patriotfront@protonmail.com jakubzak43@gmail.com

Sample responding IPs known to have been involved in the campaign include:

hxxp://188.114.99.128 hxxp://172.67.158.216 hxxp://172.67.158.171 hxxp://172.67.157.48 hxxp://50.63.202.54 hxxp://50.63.202.51 hxxp://184.168.221.37 hxxp://104.21.6.186 hxxp://50.63.202.35 hxxp://50.63.202.42 hxxp://50.63.202.39



To Historical WHOLS Red	cords [WhoisXML]	To Historical WHOIS Records (V	VhoisXML]				
2 2018-09-27 03:13:17 UTC	2018-09-24 03:13:26 UTC	2018-09-24 03:13:26 UTC	2018-05-25 02:09:47 UTC	2018-05-30 02	:09:47 UTC		
*	*	*	-	-			
patriotfront.us	patriotfront.us	patriotfront.us	patriotfront.us	patriotfro	ontus		
Registra	Registrant Email		Regiest#HtsEoriaäl/Attsfresse WHO!		egistrant Email Address KML1		
0	D			@			
cb4e16a902aaadece	e7e8a0bace9357c		jak	ubzak43@gmai	il.com		
	To Domains and	IP Aðstræðsess (Historid álPRædstrei	Salah Maring (Marine Marine Solar Salah Marine Solar Salah Marine Solar Salah Marine Solar Salah Marine Solar S	earch) [Whāis)Odi	bjains and IP Addresses (R	everse WHOIS Search) [WhoisXML
			blooda) ndsoil.us	gigabitplexus.co	m	

We'll continue monitoring the campaign and post updates as soon as new developments take place.