The Story of RaidForums

What was RaidForums?

We've spoken about a forum in the last chapter – that forum was RaidForums. Come 2022, RaidForums has also met its demise – the forum was taken off the earth after an operation by the FBI, Department of Justice, U.S. Secret Service, the Criminal Investigation division of IRS, Swedish Police, the NCA, Portuguese police, and Europol. The operation was dubbed TOURNIQUET – and it resulted in one of the world's biggest hacker forums – RaidForums – being taken down and the forum administrator and his accomplices being arrested.

The Inception of RaidForums

RaidForums was launched in 2015 – and over the years, has amassed more than half a million users. Half a million users eventually registered on RaidForums because the service has made a name for itself as *the* website that sells access to high-profile data breaches belonging to companies across a variety of industries. The forum was initially called RaidForums because its start concerned the "raiding" of Twitch channels: raiding was a coordinated activity where a group of viewers flocked to a Twitch stream to increase the viewers of a specific stream, show support, or cause disruption via trolling.

It didn't take long before RaidForums changed its direction and became a hacking forum – according to some sources, it took less than 2 years for the forum to start facilitating the sales of stolen information and start acquiring criminal hackers as part of its user base. It all started from Twitch, though.

<…>

The Entry Towards the Dark

It is speculated that many users of RaidForums have taken these steps and modified them for their use case: for many "hacking" meant something else altogether. It meant searching for the username of the streamer across a bunch of leaked databases hoping for a hit. As time went on and the users of RaidForums (and the owner himself) became older, the community of the forum realized that these kinds of things could be applied to a much wider use case. To backtrack, there was another forum related to data leaks and things more related to hacking and hackers – it went under HackForums and it was run by a man under an alias "Omniscient." Ironic, perhaps, because the Portuguese man running RaidForums elected to use the username "Omnipotent."

RaidForums had quickly become sort of a clone for HackForums: RaidForums had sort of copied the forum sections from HackForums and made similar forum sections available via RaidForums. With that said, HackForums had specific policies that disallowed black-hat hacking, fraud, and in general, crime from spreading through the forum and quickly banned users who did so, while RaidForums came up with sections that, perhaps inadvertently, facilitated discussion about such things: some of them included combo lists and discussions around them, some of them included games, but one of them became more notorious than others – it was a section titled "Databases" with a comment "Database dumps are posted here." underneath.

RaidForums and Leaked Databases

The most famous section within RaidForums included the title of "Databases." Databases, in this context, include stolen data from all kinds of websites. I've already told you what's done with these data classes – and I've also told you where hackers acquire such data. Until 2022, the primary medium to acquire such data for many was RaidForums. RaidForums has started this journey with people re-sharing leaked databases for other users of the forum to download – such databases included Adobe, Adult Friend Finder, Avast!, Ashley Madison, and others, but with time, the users of RaidForums had started incorporating hackers stealing those databases in the first place. Those hackers had started posting databases considered to be private (i.e. not yet available for other hackers and thus, having a bigger value.)

The owner of RaidForums got in on the trade as well – he'd opened an official middleman service where he'd facilitated the trade of stolen goods (databases) in return for cryptocurrency making sure no one (neither the seller nor the receiver of stolen data) gets scammed or otherwise exploited. It is said that one of the cryptocurrency addresses used by the owner of RaidForums had received over 127 bitcoins – in current prices (1 BTC = 106K USD), that would be around 13.5 million dollars. With new data breaches now reaching the forum, it had garnered the attention of both accomplished security researchers and law enforcement. RaidForums had become the main source of the latest data breaches.

<…>

The owner of RaidForums wasn't very sophisticated – a month or so after the run-in with the FBI, he was allegedly already contacting the agency in an attempt to get his seized items back. He had allegedly contacted the agency with the same email address he had used to run RaidForums with. According to various documents, the owner of the website admitted that his alias was "Omnipotent", confirmed his address in Portugal, and provided them with a picture of his ID which the FBI had quickly matched with the one from Coinbase.

What's more, the FBI agents building a case against the owner had registered on RaidForums and attempted to purchase millions of stolen credit card details from him. After a brief discussion and price negotiations, the FBI sent the money using cryptocurrency, and… got blocked as a result.

<…>

Then, in late January 2022, the owner of RaidForums flew to the United Kingdom to see his mother and was taken into custody. After that, RaidForums was made into a honeypot: everyone got logged out of the website and wasn't able to log in because everyone would be presented with an error message upon trying to do so.

Not long after that, one of the administrators of the forum – Jaw – had announced that the forum had been seized and encouraged anyone who attempted to log in to change their passwords and "clear any logs."

At first, some people thought that RaidForums got taken down by Russia, but since security researchers noticed that the nameservers of the domain had been updated to those previously used when taking down WeLeakInfo and DoubleVPN by U.S. law enforcement, it was clear that this was the job of the United States. The FBI had replaced the login page for RaidForums with a phishing page to harvest the usernames and passwords of those trying to log in, likely to peruse it in this and/or any other investigations they have going on. This has marked the end of RaidForums and it should be noted that during the course of the website's operation, the owner of RaidForums has allegedly only made around $215,571 which is a relatively small sum considering what RaidForums was known for and how it operated. Other similar websites had popped up after the incident, but they were quickly shut down as well.

Such is the nature of data breaches these days – suspicious websites often pop up often only to be quickly dismantled in the process. And no matter whether it takes days, months, or years for law enforcement to reach their goals, goals will be accomplished. And cybercriminals will bear the responsibility for their actions.

<…>