Three major hacking forums ban ransomware ads as some ransomware gangs shut down

therecord.media/three-major-hacking-forums-ban-ransomware-ads-as-some-ransomware-gangs-shut-down/

May 17, 2021

In the aftermath of the Colonial Pipeline ransomware attack, the underground cybercrime ecosystem is reshuffling, with ransomware gangs becoming pariahs.

Three hacking forums have now banned ransomware ads, three ransomware leak sites have gone down, and two other ransomware groups have announced plans to stop operating in public and go “private.”

The news comes after US President Joe Biden hinted last week in press conferences that the US would take action against ransomware gangs after the Colonial cyberattack shut down a major pipeline that transported fuel for around 45% of the US East Coast, prompting the US to trigger a rare state of national emergency.

Hacking forum bans

The first to crack under this pressure were the hacking forums, places where criminal gangs gather to advertise services, find partners, or share knowledge.

In a post from the site’s admin calling the ransomware community greedy and toxic, XSS was the first forum to ban ransomware ads last week.

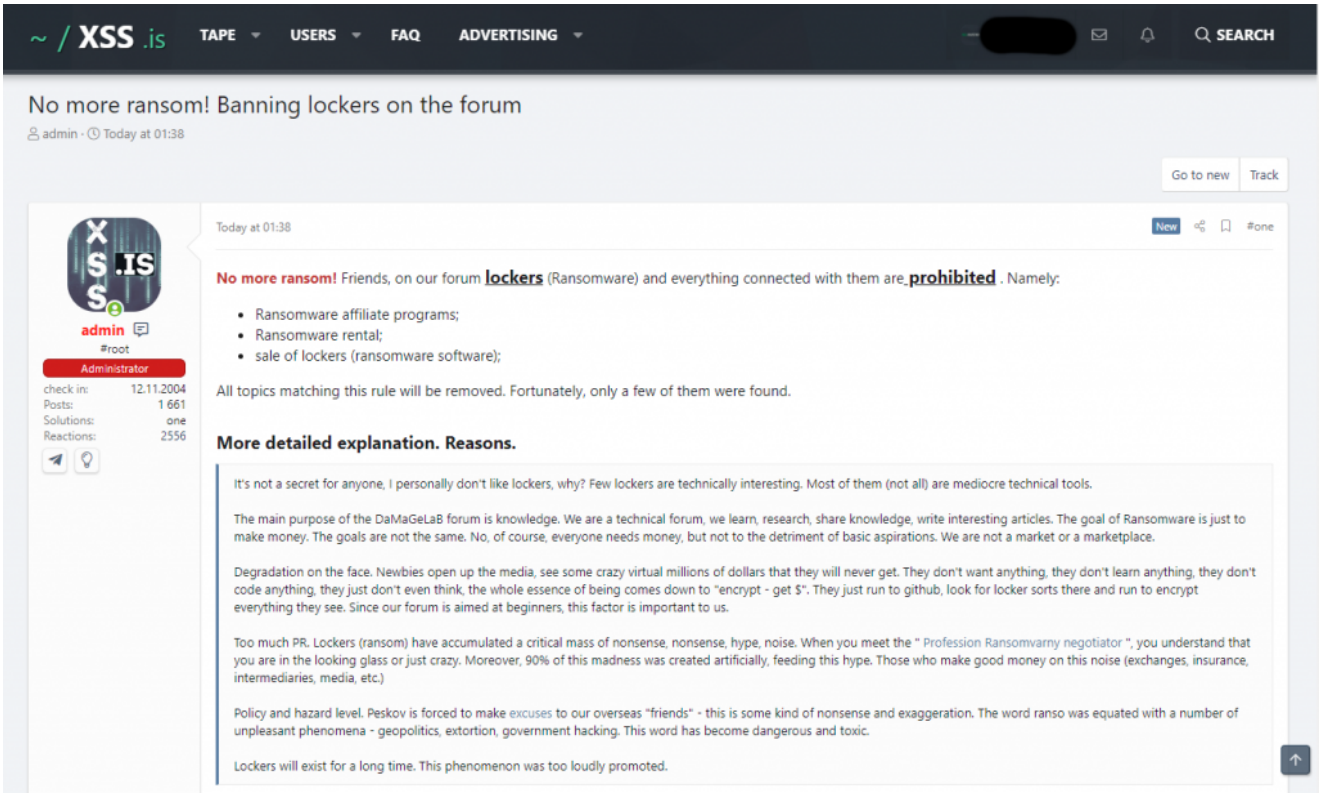

Image: The Record

A day later, the admins of the Exploit forum issued a similar ban, followed a few hours later by the operators of the RAID forum.

Image: Recorded Future

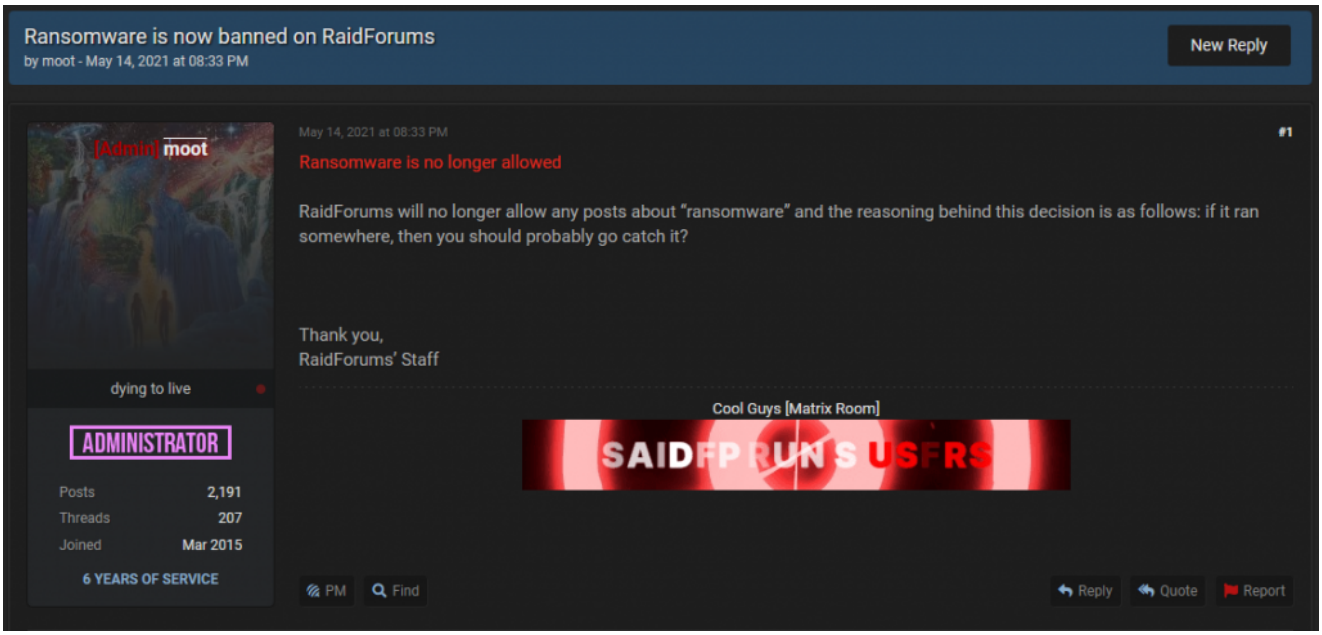

Image: The Record

The three sites are today's top destinations for most cybercrime groups and where, historically, ransomware gangs have posted and maintained forum threads advertising their services and looking for partners.

While XSS and Exploit hosted ads for the larger ransomware gangs, RAID usually hosted ads for ransomware groups entering the scene, which used the forum to create a reputation before moving to the larger XSS and Exploit.

Ransomware gangs scatter

But the forum bans on ransomware ads also signaled to ransomware gangs that their operations had crossed a line, and they reacted accordingly.

The first to go was Darkside, the ransomware gang that orchestrated the Colonial Pipeline attack. In a message posted on their website, the group said they lost control of some of their servers and some of the money they gathered from ransom payments.

While it is unclear if the group had servers taken down by US authorities or if the group performed an "exit scam," the group has abandoned its operations. Ironically, in a report published on Friday, security firm AdvancedIntelligence said that even if the Darkside group tried to stay under the radar more than any other ransomware gang, they failed by hitting the wrong target in Colonial.

But by that time, the ball got rolling. With the XSS and Exploit bans in place and with Darkside disappearing, other gangs took the hint.

Hours after Darkside went down, the operators of the REvil and Avaddon ransomware strains announced major changes to operations. In posts spotted by McAfee's John Fokker, the two ransomware gangs said they planned to stop advertising on forums altogether and

enter a “private” state, where they work with existing partners and through recommendations.

In attempts to avoid pressure from law enforcement, both groups also posted messages online claiming that they will not attack sensitive social sectors like healthcare, educational institutes, and the government networks of any country. However, if they’ll stick to these rules remains to be seen.

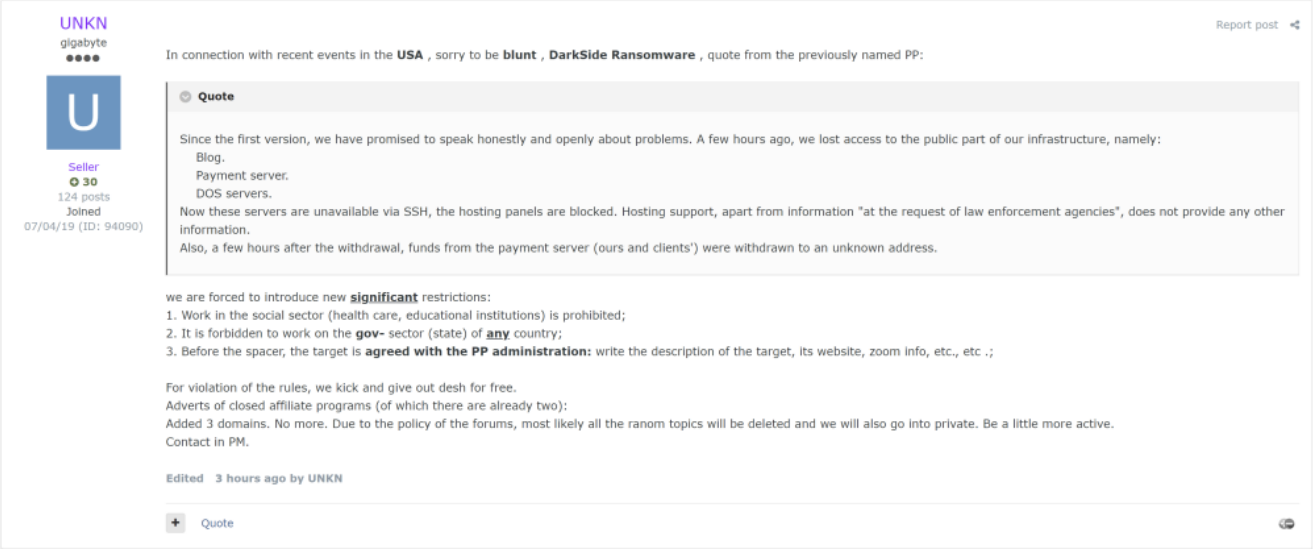

Image: Recorded Future

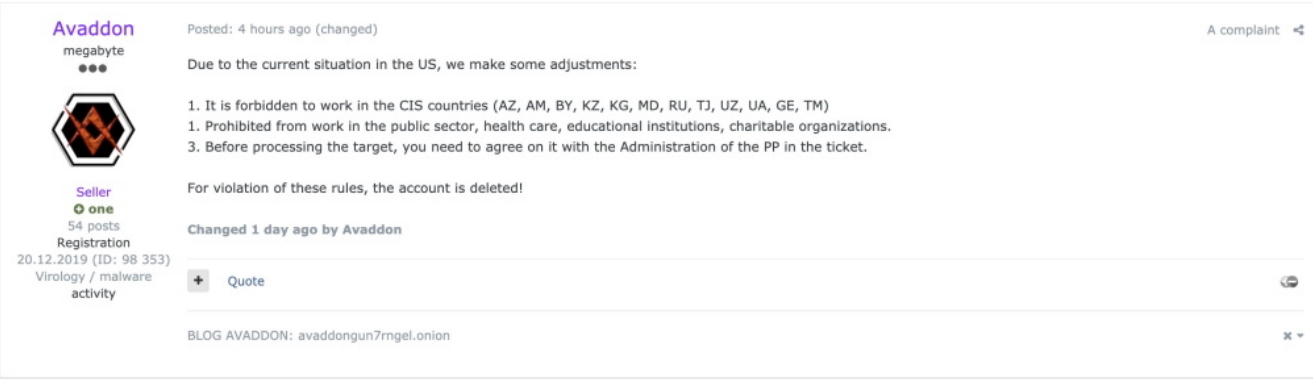

Image: John Fokker

But REvil and Avaddon went private because they had a large network of affiliates (collaborators) with which they could work and continue carrying out attacks.

Smaller groups that didn’t have similar partnerships didn’t have this option. So, over the weekend, two ransomware gangs—Ako (Razny) and Everest—appear to have chosen to shut down.

> No, I noticed the extortion site for Everest ransomware go down yesterday, but I wasn't sure if it was offline or just flaky bulletproof hosting. Yesterday I was getting some weird Google CAPTCHA stuff for AKO/RANZY, now nothing. I think we have…a thing. https://t.co/P52XaNSpXo pic.twitter.com/EKeA1seEvv
>
> — Allan “Ransomware Sommelier 🍷” Liska (@uuallan) May 16, 2021

While this reporter was told by several industry sources that there are attempts to take down some of these group's sites, the Ako site shutdown appears to be voluntary, as the gang's former site purposely redirected users to Google rather than go down as the Darkside and Everest ones.

Ransomware gangs to move into the shadows

Although some ransomware gangs appear to have now ceased operations, things are not, however, this positive. Security experts fully expect that the individuals behind these operations to continue operating in the cybercriminal underground.

Even if ransomware ads are now banned, the aforementioned forums also host ads from "initial access brokers," which sell access to "hacked networks."

This is important because, for the past year, ransomware gangs and initial access brokers have partnered and worked to orchestrate attacks together.

Just because the forums have now banned ransomware ads doesn't mean that ransomware gangs won't continue operating on these forums, and they won't reach out to initial access brokers in private and continue their partnerships, as before.

The only thing the ransomware ad ban did was to push ransomware gangs more into the shadows. They don't intend to go away. The monetary rewards are just too big, and further disruption in their ecosystem is needed, and, as some experts have suggested, more pressure needs to be applied to the cryptocurrency financial entities that often help these groups launder their profits.

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.