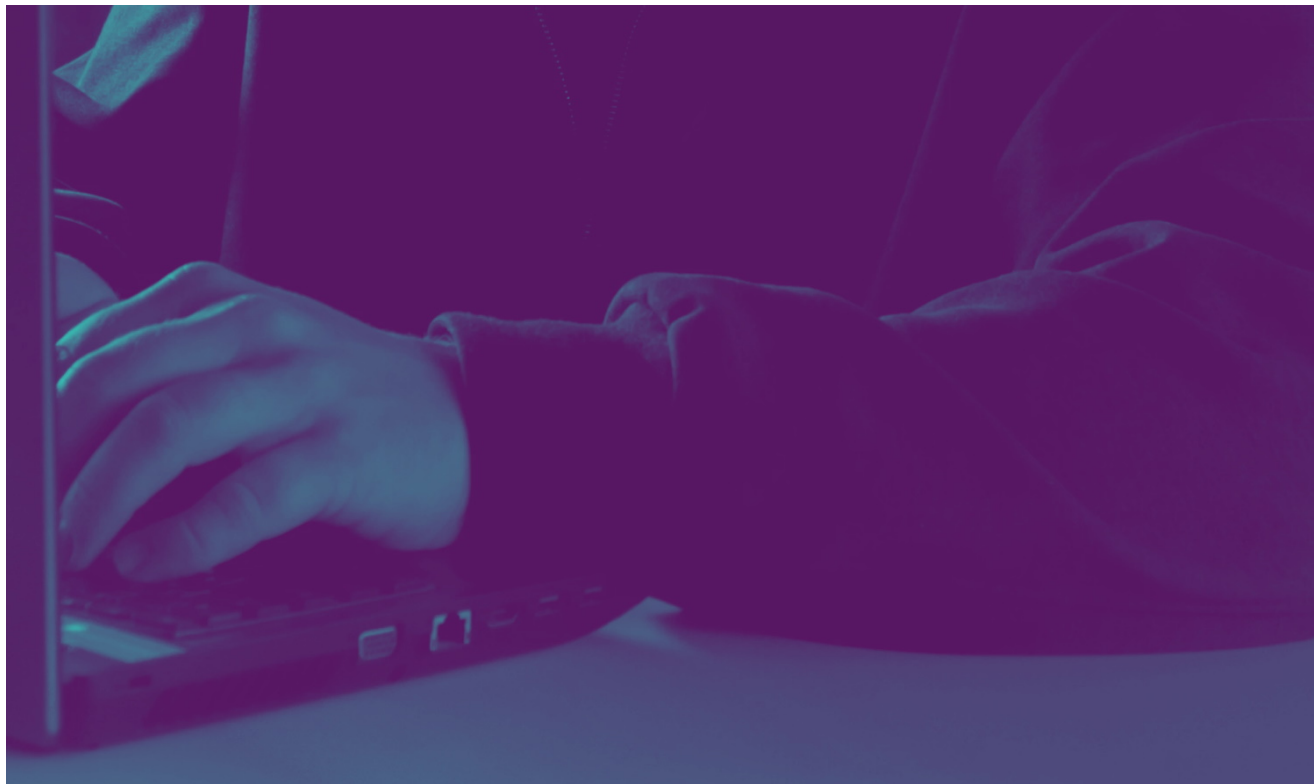


Popular hacking forum bans ransomware ads

R. therecord.media/popular-hacking-forum-bans-ransomware-ads/

May 14, 2021



One of the most popular hacking forums on the internet today announced that it would ban ransomware ads.

The XSS forum, previously known as DaMaGeLab, has been one of the two major places where ransomware gangs have advertised their services and hired partners to carry out attacks.

“Lockers (ransomware) have accumulated a critical mass of nonsense, bullshit, hype, noise,” the site’s admin said today in a post spotted by Recorded Future threat intelligence analyst and The Record author [Dmitry Smilyanets](#).

Going forward, the forum said it would prohibit ads for ransomware affiliate models and the sale or rental of ransomware strains.

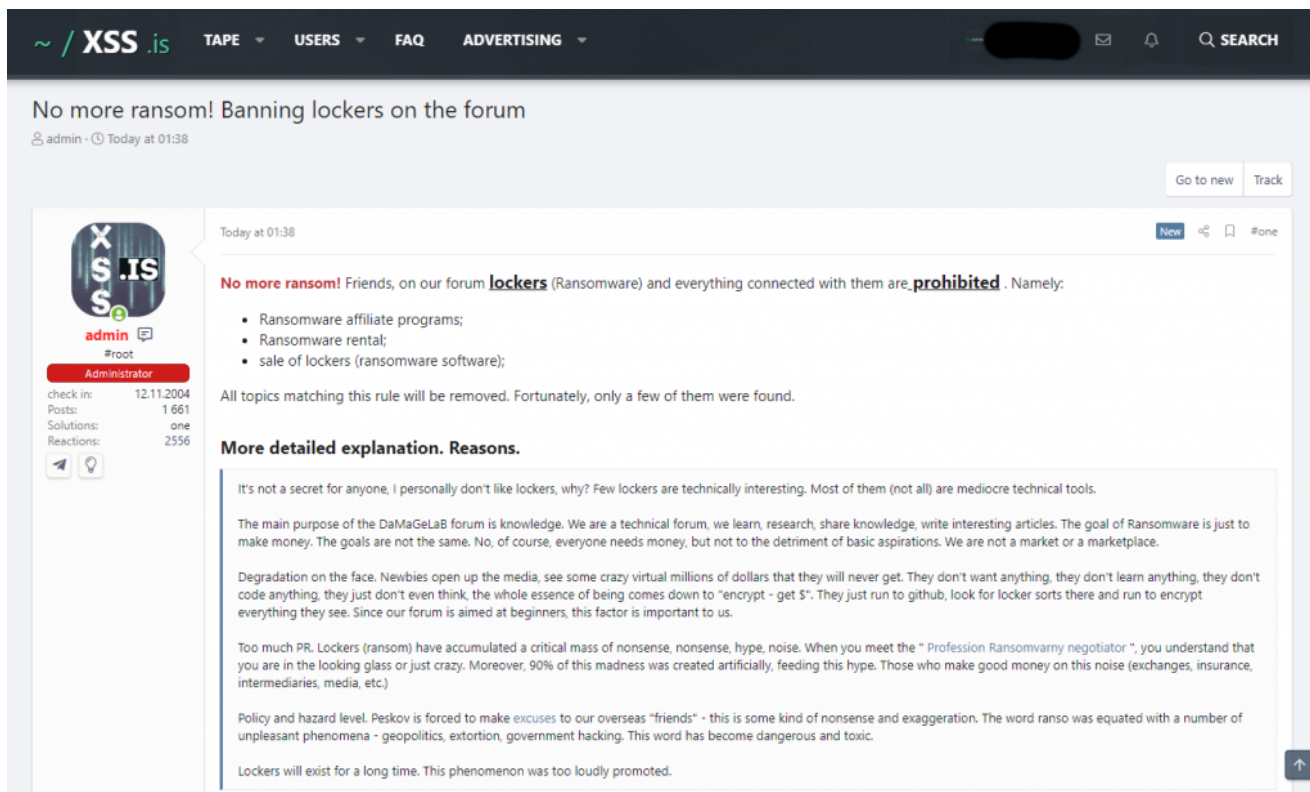


Image: The Record

The XSS ransomware ban comes after a ransomware gang known as Darkside encrypted the network of Colonial Pipeline in an attack that shut down a major pipeline that transported fuel for around 45% of the US East Coast.

The incident shone a new light on the ransomware phenomenon, which became a daily topic in White House national security briefings.

With most ransomware gangs operating out of Russia, and with most ransomware being advertised on Russian-speaking forums, industry experts expect US authorities to crack down on some of these threat actors and their enablers.

The tone appears to have been set by US President Joe Biden in a press conference on Monday, when he said that Russia has “some responsibility to deal with this [phenomenon],” before saying that he’d also bring up the topic in future discussions with Russian President Vladimir Putin.

However, even before those talks could take place, the message appears to have registered loud and clear. In a message today, the XSS admin team decided to avoid unwanted scrutiny, claiming that their forum’s main purpose was always “knowledge” and not to serve as a marketplace for criminal gangs.

Their decision might have been hastened by the fact that the Darkside ransomware gang ran an ad for its affiliate program on the XSS forum, together with all the major ransomware operations, such as REvil, Netwalker, Gandcrab, Avaddon, and many others.

Ransomware ads still allowed on Exploit

With the XSS ban today, Smilyanets expects ransomware gangs to move their recruiting and advertising operations on Exploit, another major cybercrime forum on which most gangs have also been running ads like the ones they ran on XSS.

At the time of writing, the Exploit team has not made any announcement in regards to a ransomware ad ban.

But the XSS ransomware ban today is not unique. Cybercrime forum admins have often banned certain topics on their sites when they believed law enforcement might take them in their sights.

For example, in 2016, after a hacker published the source code of the Mirai DDoS botnet on HackForums, the site's admin responded by banning DDoS-for-hire service ads a few days later, not wanting to be in the crosshairs of an FBI investigation looking into a series of Mirai DDoS attacks that crippled large parts of the internet.

Similarly, when internet pranksters started hacking into Zoom meetings and recording users in early 2020, forums like Cracked and Nulled, where pranksters often went to organize or request Zoom bombing sessions, banned the posting of any Zoom-related content on their sites.

UPDATED on May 14, 16:30pm: A day after the XSS forum banned ransomware ads, the Exploit forum followed suite and also announced a similar decision. Currently, both of the two major hacking forums where ransomware ads were being posted have banned these types of adverts on their sites.

Another one bites the dust – forum Exploit bans [#ransomware](https://twitter.com/d4nknltz7E)
[pic.twitter.com/d4nknltz7E](https://twitter.com/d4nknltz7E)

— Dmitry Smilyanets (@ddd1ms) [May 14, 2021](#)

Tags

- [cybercrime](#)
- [DaMaGeLaB](#)
- [Darkside](#)
- [forum](#)
- [hacking forum](#)
- [Ransomware](#)
- [ransomware ad](#)
- [XSS](#)

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.