Popular Russian hacking forum XSS bans all ransomware topics

bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

Lawrence Abrams

By
Lawrence Abrams

- May 13, 2021
- 09:48 PM
- 2

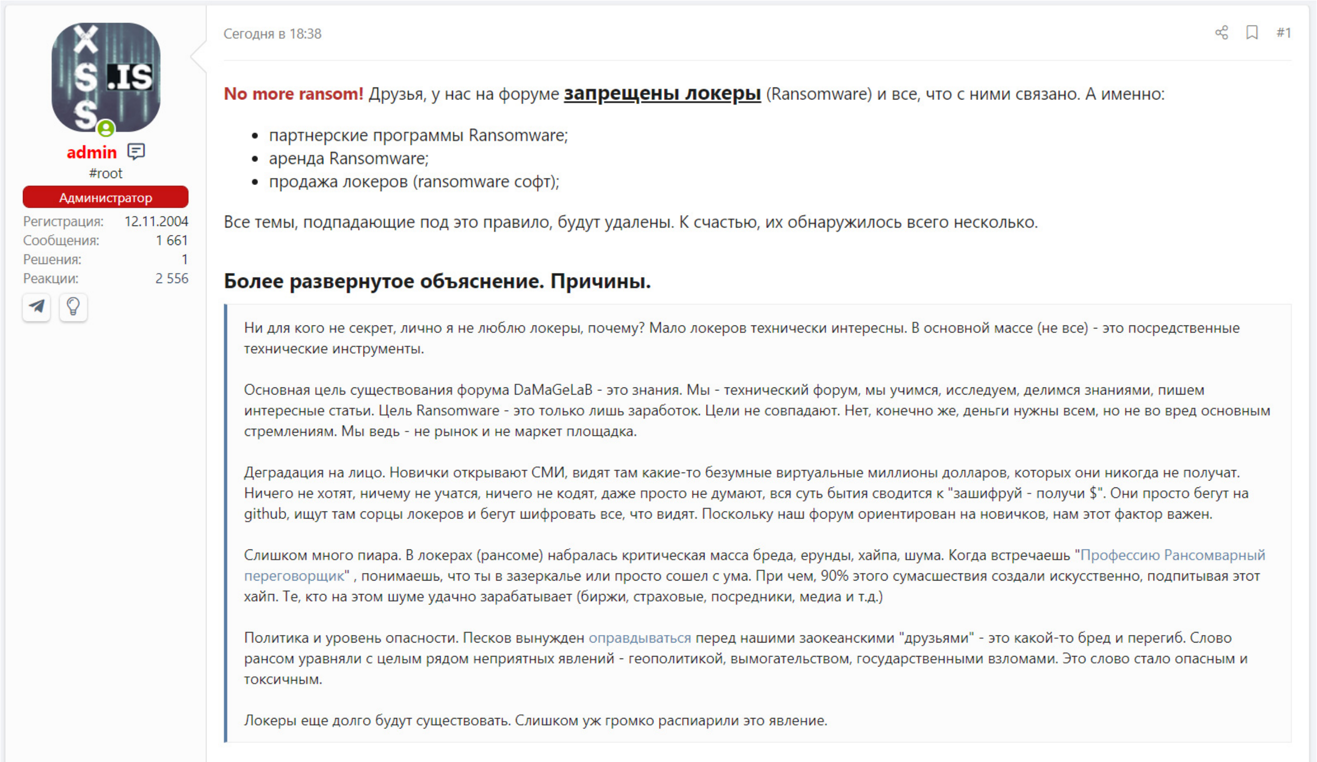
One of the most popular Russian-speaking hacker forums, XSS, has banned all topics promoting ransomware to prevent unwanted attention.

XSS is a Russian-speaking hacking forum created to share knowledge about exploits, vulnerabilities, malware, and network penetration.

With the rise of ransomware, Ransomware-as-a-Service (RaaS) gangs, such as REvil, LockBit, DarkSide, Netwalker, Nefilim, have increasingly been using the forum to enlist new affiliates/partners to their operation.

After DarkSide encrypted Colonial Pipeline and disrupted the U.S. fuel pipeline's operation, law enforcement and security researchers have been increasingly scrutinizing the ransomware gang and sites that promote it.

In a forum post discovered by Advanced Intel's Yelisey Boguslavskiy, the owner of the XSS hacking forum, known as 'Admin,' posted today that forum topics promoting ransomware are no longer allowed at the site.



admin

#root

Администратор

Регистрация: 12.11.2004

Сообщения: 1 661

Решения: 1

Реакции: 2 556

Сегодня в 18:38

#1

No more ransom! Друзья, у нас на форуме **запрещены локеры** (Ransomware) и все, что с ними связано. А именно:

- партнерские программы Ransomware;
- аренда Ransomware;
- продажа локеров (ransomware софт);

Все темы, подпадающие под это правило, будут удалены. К счастью, их обнаружилось всего несколько.

Более развернутое объяснение. Причины.

> Ни для кого не секрет, лично я не люблю локеры, почему? Мало локеров технически интересны. В основной массе (не все) - это посредственные технические инструменты.
>
> Основная цель существования форума DaMaGeLaB - это знания. Мы - технический форум, мы учимся, исследуем, делимся знаниями, пишем интересные статьи. Цель Ransomware - это только лишь заработок. Цели не совпадают. Нет, конечно же, деньги нужны всем, но не во вред основным стремлениям. Мы ведь - не рынок и не маркет площадка.
>
> Деградация на лицо. Новички открывают СМИ, видят там какие-то безумные виртуальные миллионы долларов, которых они никогда не получат. Ничего не хотят, ничему не учатся, ничего не кодят, даже просто не думают, вся суть бытия сводится к "зашифруй - получи $". Они просто бегут на github, ищут там сорцы локеров и бегут шифровать все, что видят. Поскольку наш форум ориентирован на новичков, нам этот фактор важен.
>
> Слишком много пиара. В локерах (рансоме) набралась критическая масса бреда, ерунды, хайпа, шума. Когда встречаешь "Профессию Рансомварный переговорщик" , понимаешь, что ты в зазеркалье или просто сошел с ума. При чем, 90% этого сумасшествия создали искусственно, подпитывая этот хайп. Те, кто на этом шуме удачно зарабатывает (биржи, страховые, посредники, медиа и т.д.)
>
> Политика и уровень опасности. Песков вынужден оправдываться перед нашими заокеанскими "друзьями" - это какой-то бред и перегиб. Слово рансом уравняли с целым рядом неприятных явлений - геополитикой, вымогательством, государственными взломами. Это слово стало опасным и токсичным.
>
> Локеры еще долго будут существовать. Слишком уж громко распиарили это явление.

Forum post banning ransomware topics

This post states that all "Ransomware affiliate programs", "Ransomware rental", and the "sale of lockers (ransomware software)" are prohibited, and any existing topics will be deleted.

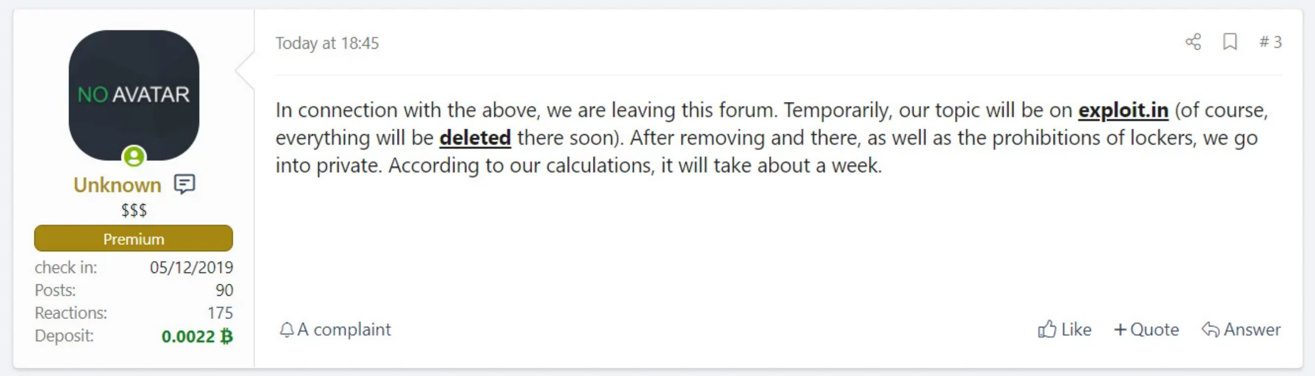
The reason for the ban is that the owner feels that ransomware brings unwanted attention to the site and "has become dangerous and toxic."

You can read a portion of the translated text below:

> "Degradation on the face. Newbies open up the media, see some crazy virtual millions of dollars that they will never get. They don't want anything, they don't learn anything, they don't code anything, they just don't even think, the whole essence of being comes down to "encrypt - get $". They just run to github, look for locker sorts there and run to encrypt everything they see. Since our forum is aimed at beginners, this factor is important to us.
>
> Too much PR. Lockers (ransom) have accumulated a critical mass of nonsense, nonsense, hype, noise. When you meet the " Ransomvarny negotiator " Profession , you understand that you are in the looking glass or just crazy. Moreover, 90% of this madness was created artificially, feeding this hype. Those who make good money on this noise (exchanges, insurance, intermediaries, media, etc.)
>
> Policy and hazard level. Peskov is forced to make excuses in front of our overseas "friends" - this is some kind of nonsense and exaggeration. The word ranso was equated with a number of unpleasant phenomena - geopolitics, extortion, government hacking. This word has become dangerous and toxic.
>
> Lockers will exist for a long time. This phenomenon was too loudly promoted."

Ransomware gangs not happy

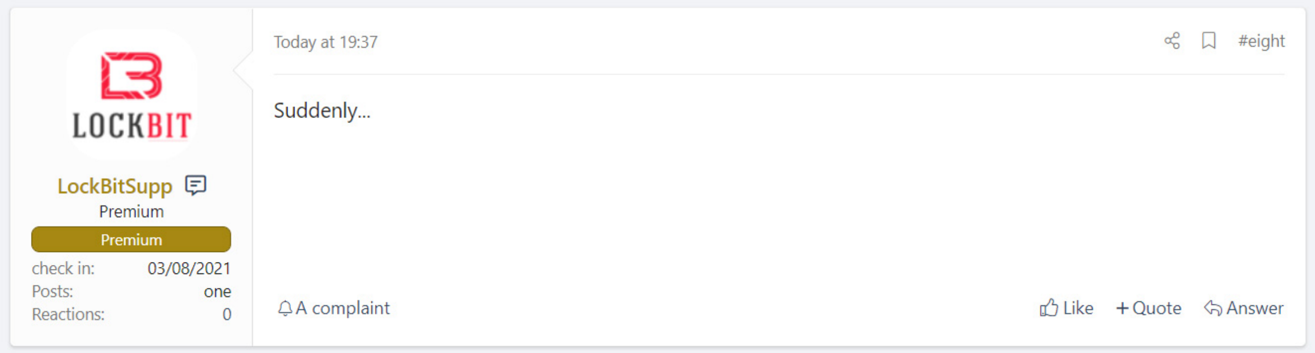
Shortly after the posting of the topics, representatives of the REvil ransomware gangs showed their displeasure.



Today at 18:45 # 3

In connection with the above, we are leaving this forum. Temporarily, our topic will be on **exploit.in** (of course, everything will be **deleted** there soon). After removing and there, as well as the prohibitions of lockers, we go into private. According to our calculations, it will take about a week.

Post by REvil representative



Today at 19:37 #eight

Suddenly...

Post by LockBit operator

With ransomware gang's core members keeping a low profile, law enforcement targets the affiliates to weaken or force an operation to close down.

As more hacking communities make ransomware operations unwelcome, it will become harder for RaaS operations to recruit new affiliates and promote their activities.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

Screencastify Chrome extension flaws allow webcam hijacks

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.