






THE LATEST INDUSTRY WEBINARS
NOW ON DEMAND

Watch now

Sign UpLog In



info security
STRATEGY | INSIGHT | TECHNOLOGY


Latest
Marine Charged with Cyber-Stalking

INFOSECURITY MAGAZINE HOME » NEWS » CYBERCRIME FORUM BANS RANSOMWARE ACTIVITY

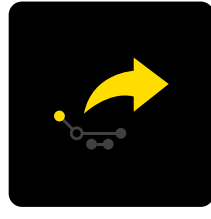
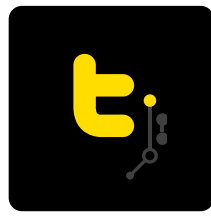



17 MAY 2021NEWS

Cybercrime Forum Bans Ransomware Activity



Phil MuncasterUK / EMEA News Reporter, Infosecurity Magazine
Email PhilFollow @philmuncaster



A popular cybercrime forum claims to have banned all ransomware activity due to ideological differences and concerns over the amount of publicity that high-profile incidents are generating.

Russian language forum XSS has contributed to the success of Ransomware as a Service (RaaS) groups like Netfilim, REvil, DarkSide and Babuk, by providing a platform to recruit new affiliates, according to [Flashpoint](#).

However, an administrator post late last week claimed that all sales of ransomware and affiliate activity would be prohibited from the site, the threat intelligence vendor reported.

The activity of groups like DarkSide, which recently caused a furore after disrupting fuel supplies on the [US East Coast](#), are generating “too much PR,” escalating geopolitical and law enforcement risk and building a “critical mass of nonsense, hype, and noise,” according to the post.

The geopolitical aspect appears significant: the post apparently argues that when President Putin’s press secretary has to deny Kremlin involvement in attacks, “this is a bit too much.”

Russian cyber-criminals have always been sheltered by the state on the unwritten proviso that attacks are aimed at the country’s strategic foes, such as European and North American countries.

XSS’s decision would seem to suggest some in the community are becoming anxious at the level of scrutiny from the US and other governments that such attacks are drawing.

Flashpoint also claimed that DarkSide released a now-deleted statement claiming that its data leak blog, payment server and DOS servers have been blocked and funds from the payment servers were “withdrawn to an unknown address.”

However, according to a statement from [Digital Shadows](#), forum members have questioned the authenticity of the post.

In the meantime, it’s unlikely that XSS’s decision will impact the ransomware industry.

“Flashpoint assesses with moderate confidence that well-established ransomware collectives — including REvil, LockBit, Avaddon, and Conti — will continue to operate in private mode,” [the vendor said](#).

“Additionally, ransomware collectives will likely begin to advertise recruitment for new affiliates via their own leak sites since many cyber-criminal forums, like XSS, and other similar platforms used for ransomware advertisements will now likely refuse to host their activities.”



Online Summit
INFOSECURITY MAGAZINE
22-23 MARCH 2022
14 SESSIONS 11 CPES 2 DAYS
Unlock Learnings & Network with the Global Cybersecurity Community
REGISTER NOW

Related to This Story

- DoJ Seizes Millions in Ransom Paid by Colonial Pipeline to Darkside Hackers
- Colonial CEO Reportedly Confirms \$4.4 Million Ransom Payment
- Toshiba Business Reportedly Hit by DarkSide Ransomware
- Colonial Pipeline Attackers Linked to Infamous REvil Group
- US Offers \$10m Reward to Unmask DarkSide Leaders

What’s Hot on Infosecurity Magazine?

ReadSharedWatchedEditor's Choice

1

8 JUL 2021NEWS

New PrintNightmare Patch Can Be Bypassed, Say Researchers

2

8 JUL 2021NEWS

Cybercrime Costs Organizations Nearly \$1.79 Million Per Minute

3

8 JUL 2021NEWS

CTOs Keeping Quiet on Breaches to Avoid Cyber Blame Game

4

7 JUL 2021NEWS

Over 170 Scam Cryptomining Apps Charge for Non-Existent Services

5

7 JUL 2021NEWS

Most Insider Data Breaches Aren’t Malicious

6

7 JUL 2021NEWS

Kremlin Hackers Reportedly Breached Republican National Committee

ALSO ON INFOSECURITY MAGAZINE

#DataPrivacyWeek: Prioritize Data ...

20 days ago • 1 comment

Organizations must re-evaluate their data protection strategies ...

US and Israel Agree Anti-Ransomware ...

3 months ago • 1 comment

Bilateral deal comes as part of cyber taskforce launch


Crypto Fin Rug from

a month ago •

Arbix Financ make off with

0 CommentsInfosecurity MagazinePrivacy Policy





FavoriteTweetShareSort by Best



Start the discussion...

LOG IN WITH

info security



OR SIGN UP WITH DISQUS

Name

Email

Password

☐ I agree to Disqus' [Terms of Service](#)

☐ I agree to Disqus' processing of email and IP address, and the use of cookies, to facilitate my authentication and posting of comments, explained further in the [Privacy Policy](#)

☐ I agree to additional processing of my information, including first and third party cookies, for personalized content and advertising as outlined in our [Data Sharing Policy](#)

→

Be the first to comment.

SubscribeAdd DisqusDo Not Sell My Data

DISQUS

The Magazine
About Infosecurity
Subscription
Meet the Team
Contact Us



Unlock Learnings & Network with the Global Cybersecurity Community

14 SESSIONS 2 DAYS
11 CPES

REGISTER NOW



infosecurity
CONNECTING THE INDUSTRY IN PERSON, IN PRINT, ONLINE

- Advertisers
Media Pack
- Contributors
Forward Features
Op-ed
Next-Gen Submission