

New Operators Usurp Elite Russian Hacker Forum "Verified"

 flashpoint-intel.com/blog/new-mysterious-operators-usurp-elite-russian-hacker-forum-verified/

February 22, 2021



Blogs

Blog

New Mysterious Operators Usurp Elite Russian Hacker Forum "Verified"

On February 17, 2021, the elite Russian hacker forum, "Verified," resurfaced abruptly, stood up with new web domains and new, unnamed admins claiming ownership. The speed and erratic nature of these developments, along with the peculiar nature of the new admins' communications, have left many cybercriminal users suspicious as to the operators' real intentions and credibility.

Frenetic Takeover of "Verified" Hacker Forum Leave Cybercriminals Wary

On February 17, 2021, the elite Russian hacker forum, "Verified," resurfaced abruptly, stood up with new web domains and new, unnamed admins claiming ownership. The speed and erratic nature of these developments, along with the peculiar nature of the new admins'

communications, have left many cybercriminal users suspicious as to the operators' real intentions and credibility.

Flashpoint analysts continue to investigate the Verified forum and are actively monitoring hacker chatter for any noticeable shifts in community behavior or sentiment.

Notorious Russian Hacker Forum Active for More Than a Decade

For well over a decade now, Verified has been among the top cybercriminal venues for highly-skilled Eastern European hackers and associates, who routinely flock to the site to conduct their illicit cyber operations.

New, Unnamed Operators Gain Control, Promise Changes

As new Verified-linked domains emerged online last week, an unknown group of nameless administrators claimed to usurp control of the long-standing forum. Following their successful takeover, the new admins notified all Verified forum users of this news, making use of the previous admin alias "VR_Support" to alert the entire forum community. They explained the reason for their abrupt takeover, claiming that the prior admins locked them out of Verified's former domains. Upon gaining access to Verified's admin panel, they allegedly found the forum's networking infrastructure in disarray with little to no security or user protections of note.

The new operators purport that Verified's inadequate site security propelled them into action to seize control, further asserting that the former site domain (verified[.jsc) had been hacked. They promised to share screenshots as proof, but as of the writing of this post, that evidence has yet to materialize.

Dubious Timing and No New Inventory Add to Cybercriminal Suspicions

The new admins also announced additional operational changes to the forum: They plan to deactivate the forum's former Jabber support servers and will offer free registration to all users for an extended period of time to encourage swift adoption of the new domains. While the renewed flurry of admin activity may reassure some cybercriminal users, many remain skeptical due to the dubious timing of it all and the lack of new forum data since January 20, 2021—which, coincidentally or not, is the same date as the site's claimed seizure and ownership transfer.

Former Verified Operators' Continued Silence Is Deafening

Further confounding forum users and cybercriminal onlookers alike, the former admins of the old Verified domain have not yet acknowledged the seizure and transfer of Verified anywhere online. No one has even copped to connectivity issues or other technical malfunctions that

act at least as a partial explanation for all of this frantic movement.

Cybercriminal Suspicion Loud and Well-Founded

Needless to say, the frenetic pace of activity and the suspect narrative meant to ease user trepidation may have done just the opposite, deepening their concerns rather than alleviating them. Some savvy Verified cybercriminal users clearly have their eyebrows raised as they comment on the new admins' posts with skeptical reactions, mentions of "fake news," and expletive-laden posts trolling the new management.

Users on the rival Russian-language hacker forum "Exploit" have also expressed their own disbelief about the dubious Verified domain and administration changes. In the wake of several recent [high-profile US-EU joint law enforcement campaigns](#) targeting other prominent Eastern European cybercriminal syndicates and illicit dark web marketplaces with operations stemming back to places like Bulgaria and Ukraine—perhaps, these suspicions are well-justified.

See Flashpoint Intelligence in Action

Why wait? [Sign up for your 90-day risk-free trial, today!](#) Experience firsthand how Flashpoint Intelligence offerings support leading security and fraud teams worldwide on a daily basis and during their most critical times.

In a matter of minutes, you'll see why Flashpoint delivers [482% ROI](#) with a three-month payback period, and how we take your team and entire program to the next level.