

 BRIEF

Anonymous Deep Web Expansion Met with Skepticism

ZEROFOX INTELLIGENCE

B-2022-03-29a

Classification: TLP White

Criticality: High

Intelligence Requirements: Deep Dark Web & Criminal Underground

March 29, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:40 PM (EDT) on March 29, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Anonymous Deep Web Expansion Met with Skepticism

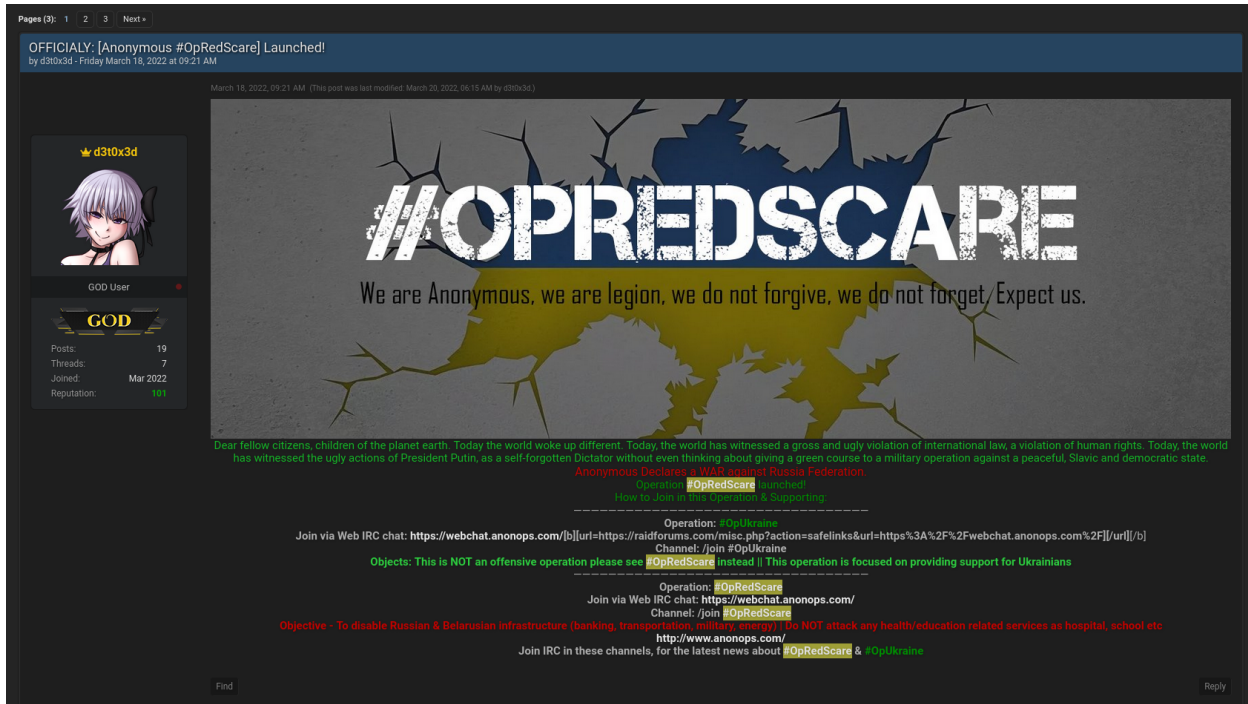
Executive Summary

On March 18, 2022, hacktivist group Anonymous posted a call to arms on a deep web forum to disable Russian and Belarusian infrastructure that they dubbed #OpRedScare. Responses to the post indicate that active underground community members are critical of Anonymous' mission, techniques and tradecraft. However, the resulting chatter clearly showed that those in the pro-Ukraine camp continue to support taking disruptive cyber actions against Russia, Russia-based entities, and businesses they judge are too supportive of Russia.

Analyst Commentary

On March 18, 2022, forum member "d3t0x3d," who is also allegedly a member of hacktivist group Anonymous, posted a call to arms on the Deep Web forum breached[.]co (the heir apparent to the now-defunct RaidForums) dubbed #OpRedScare. This new offensive campaign's stated objectives are to "disable Russian and Belarusian infrastructure (banking, transportation, military, energy)," but Anonymous has specified that education and healthcare-related entities should be left alone. The post unleashed the ire of fellow underground cyber actors critical of Anonymous' mission, techniques, and tradecraft.

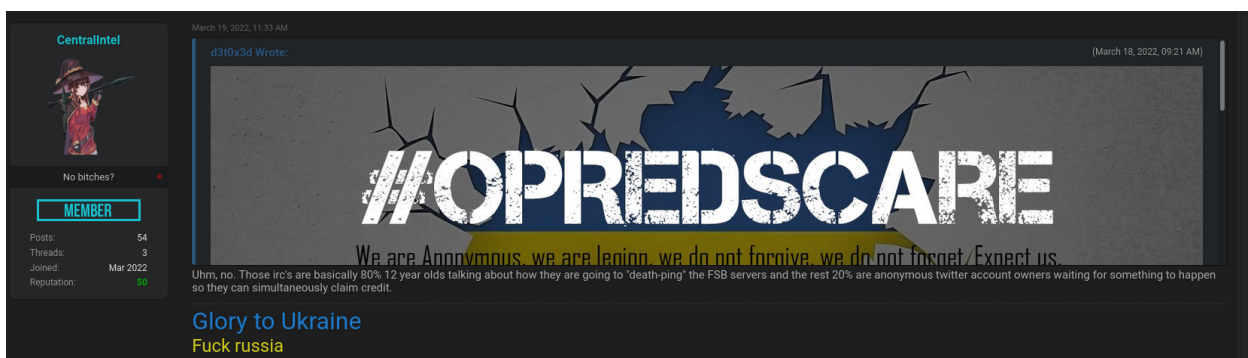
The post provided a link to an IRC chat for those interested in joining the campaign, as well as a link to a new thread on March 23, 2022, where Anonymous would provide updates on the campaign's progress; as of this writing, no updates have been posted.



Source: breached[.]co

d3t0x3d's original post regarding #OpRedScare campaign

Multiple breached[.]co forum members have criticized the claims made within the #OpRedScare thread. Breached[.]co forum member "CentralIntel" replied to the thread stating that the Anonymous IRC chat(s) consist of "80% 12 year olds... and 20% are anonymous twitter account owners waiting for something to happen so they can simultaneously take credit." Extremely well-regarded forum member "Minori" agreed with CentralIntel's comment replying "sadly true."



Source: breached[.]co

CentralIntel's breach[.]co forum profile highlights eager support for Ukraine

Another well-regarded forum member "Holistic-Killer" replied that Anonymous is "always creating cool images and taking credit for some other people's work. They still

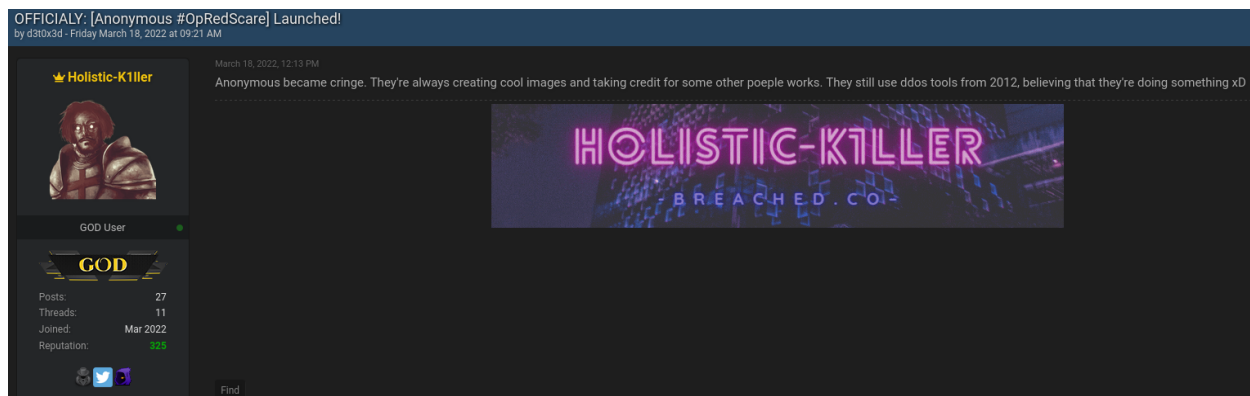


use ddos [sic] tools from 2012...” further demonstrating the discontent active underground community members feel for Anonymous.



Source: breached[.]co

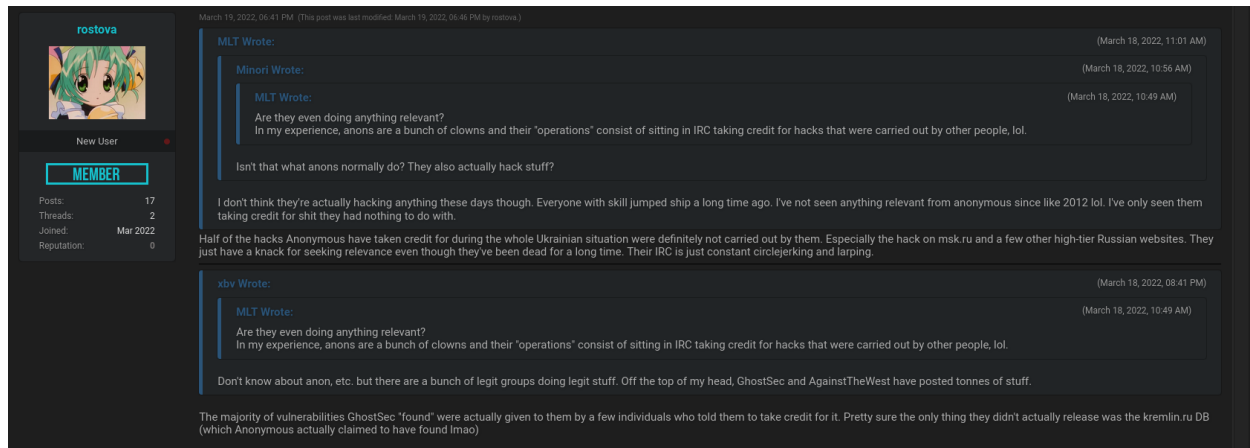
Chatter between CentralIntel and Minori regarding the #OpRedScare campaign and Anonymous



Source: breached[.]co

Reply by Holistic-K1ller regarding the #OpRedScare campaign and Anonymous

Although skepticism surrounding Anonymous persists, underground actors within the pro-Ukraine camp continue to support calls to take disruptive cyber actions against Russia, Russia-based entities, and businesses they judge are too supportive of Russia. Robust chatter on the #OpRedScare thread between threat actors indicates that groups such as GhostSec and AgainstTheWest are held in higher esteem than Anonymous—especially regarding actions taken against Russia—and are still firmly committed to actions on behalf of Ukraine and against Russia.



Source: [breached\[.\]co](#)

Chatter between forum members regarding groups taking actions against Russia



Appendix: Traffic-Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

TLP:

WHITE information may be distributed without restriction, subject to copyright controls.