

A logo consisting of a white globe with a lightning bolt symbol inside, representing the 'FLASH' brand.

FLASH

The Significance of Pro-Russian Killnet Group's Leadership Change

ZEROFOX INTELLIGENCE

F-2022-08-08a

Classification: TLP:White

Criticality: High

Intelligence Requirements: PII & Fraud, Deep Dark Web & Criminal Underground

August 8, 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 8:00 AM (EDT) on August 8, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

The Significance of Pro-Russian Killnet Group's Leadership Change

Key Findings

The announcement of a leadership change for pro-Russian threat actor group “Killnet” comes after the seemingly incoherent messaging around Killnet’s alleged intrusion into Lockheed Martin and the as-yet-unproven claims that the group is responsible. Killnet’s newly-named leader’s reputation as a skilled ransomware operator suggests a pivot to a more professional hack and dump operation and a potential escalation in information warfare directed at pro-Ukraine governments and businesses.

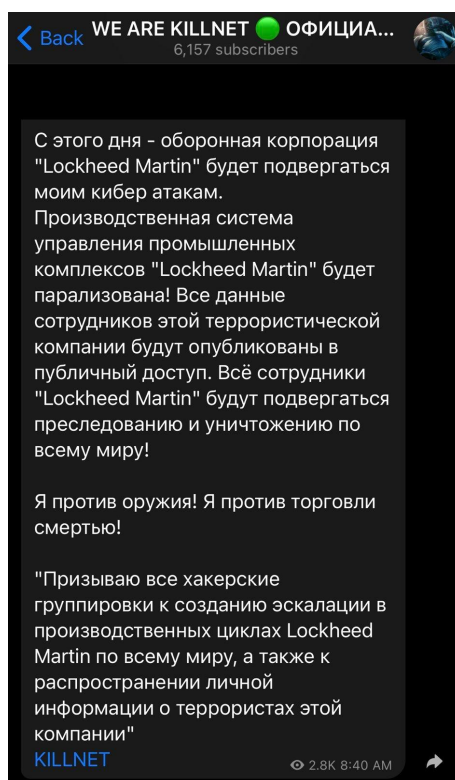
Analyst Commentary

Killnet has been one of the most vocal threat actor groups since the start of Russia’s invasion of Ukraine. The pro-Russian hacktivist collective, identified as early as January 2022, initially sold Distributed Denial of Service (DDoS) tools as part of a subscription model. Killnet changed tactics from a cybercriminal service provider to a hacktivist group in February 2022, when it declared war on the Anonymous hacking collective after Anonymous expressed public support for Ukraine.

Killnet’s scope of targets has since expanded to include numerous countries that oppose Russia or support Ukraine, including NATO members. Attacks typically target the websites of government agencies, critical infrastructure, financial institutions, and transport hubs. The goal of these attacks is to take victims’ websites offline and impact the economy of targeted countries while embarrassing the victim. Killnet’s organization appears structured, with lines of command and tasking for operative groups. Its primary means of communication is via Telegram, where the group has more than 100,000 subscribers across its channels. Killnet’s attacks are typically announced on the group’s Telegram channels prior to occurring,



Recently and very notably, the group's founder and leader, "KillMilk," announced that he was leaving Killnet.¹ KillMilk appears to have moved on to different channels, indicating that the actor likely has not retired. Killnet's newly-named leader has a reputation for being a skilled ransomware operator, suggesting a pivot to a more professional hack and dump operation and a potential escalation in information warfare directed at pro-Ukraine governments and businesses. The newly-announced successor goes by the handle "BlackSide" and will replace "KillMilk" at a heretofore undetermined time, judging from media reporting and Killnet's official Telegram channel.²³



Killnet's Claim Regarding Hacking Lockheed Martin

Source: ZeroFox Intelligence

BlackSide is reportedly an admin of an exclusive, closed Dark Web forum and has an extensive background in ransomware, phishing, and cryptocurrency exchange theft;⁴ BlackSide's résumé and admin status suggest a well-regarded and competent actor with

¹

[hXXps://www.scmagazine\[.\]com/analysis/cybercrime/founder-of-pro-russian-hackivist-killnet-quitting-group](https://www.scmagazine.com/analysis/cybercrime/founder-of-pro-russian-hackivist-killnet-quitting-group)

² [hXXps://www.pwndefend\[.\]com/2022/05/18/killnet-area-they-really-a-threat/](https://www.pwndefend.com/2022/05/18/killnet-area-they-really-a-threat/)

³ [hXXps://t\[.\]me/killnetj](https://t.me/killnetj)

⁴

[hXXps://www.scmagazine\[.\]com/analysis/cybercrime/founder-of-pro-russian-hackivist-killnet-quitting-group](https://www.scmagazine.com/analysis/cybercrime/founder-of-pro-russian-hackivist-killnet-quitting-group)



extensive connections to the Russian underground cyber community and official Russian state intelligence or law enforcement agencies. Killnet was founded by KillMilk, is a vehement supporter of Russia's war in Ukraine,⁵ and has been perceived as less professional and successful than its pro-Ukraine rival, the I.T. Army of Ukraine.⁶⁷

The announcement of the leadership change comes after the seemingly incoherent messaging around Killnet's alleged intrusion into Lockheed Martin and the as-yet-unproven claims the group is responsible. Additionally, it is not uncommon for Killnet to claim responsibility for attacks that it did not carry out in an attempt to increase its notoriety; the addition of a credible actor like BlackSide will likely reduce the need for such tactics.

ZeroFox Intelligence notes that the Russian-speaking cyber underground is intentionally murky, with complicated and blurry alliances between groups and government agencies that are both informal and formal. Most hacktivist groups in Russia have permission to operate from a "krysha"—a person of influence within an official government apparatus that blesses and protects the group and its activities. In this particular case, it appears that the mishandling of the public messaging behind the alleged high-profile Lockheed Martin data heist crossed a blurred and often invisible line, which may have forced KillMilk to resign and pass the reins to a more competent practitioner of the cyber dark arts.

Recommendations

Organizations should ensure that monitoring is configured on Killnet's Telegram channels for any mentions of their domains or any other organizational mentions. In addition, given the ransomware expertise of BlackSide, organizations should be extremely mindful of signs of ransomware activity, such as spikes in disk activity, suspicious emails, and/or unauthorized access to the active directory, as Killnet is highly likely to continue targeting pro-Ukraine governments and businesses.

⁵ [hXXps://www.pwndefen\[.\]com/2022/05/18/killnet-area-they-really-a-threat/](https://www.pwndefen[.]com/2022/05/18/killnet-area-they-really-a-threat/)

⁶

[hXXps://www.scmagazine\[.\]com/analysis/cybercrime/founder-of-pro-russian-hacktivist-killnet-quitting-group](https://www.scmagazine[.]com/analysis/cybercrime/founder-of-pro-russian-hacktivist-killnet-quitting-group)

⁷ [hXXps://www.wired\[.\]com/story/ukraine-it-army-russia-war-cyberattacks-ddos/](https://www.wired[.]com/story/ukraine-it-army-russia-war-cyberattacks-ddos/)



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.