

Cyber Shadows Pact: Darknet Parliament (KillNet, Anonymous Sudan, REvil)

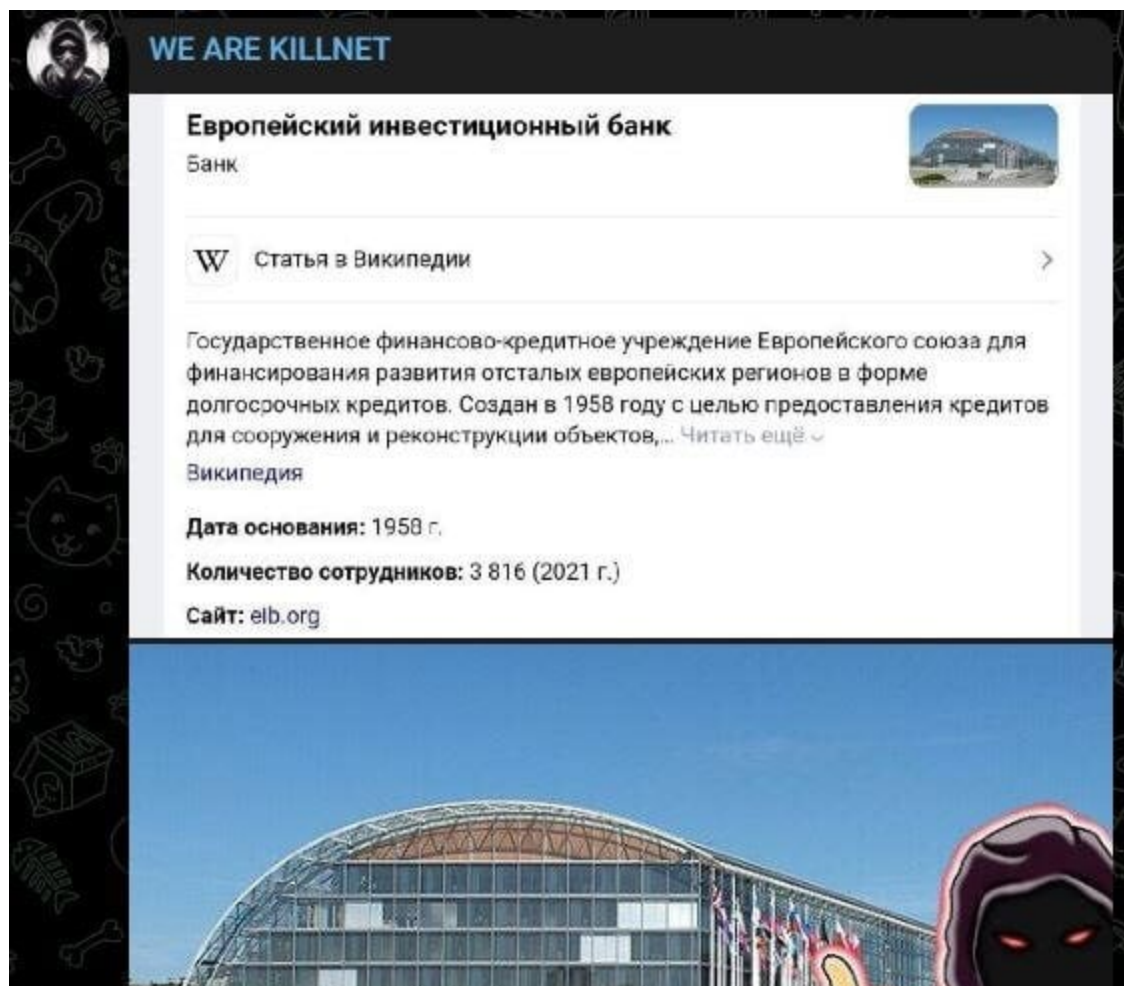
 socradar.io/cyber-shadows-pact-darknet-parliament-killnet-anonymous-sudan-revil/

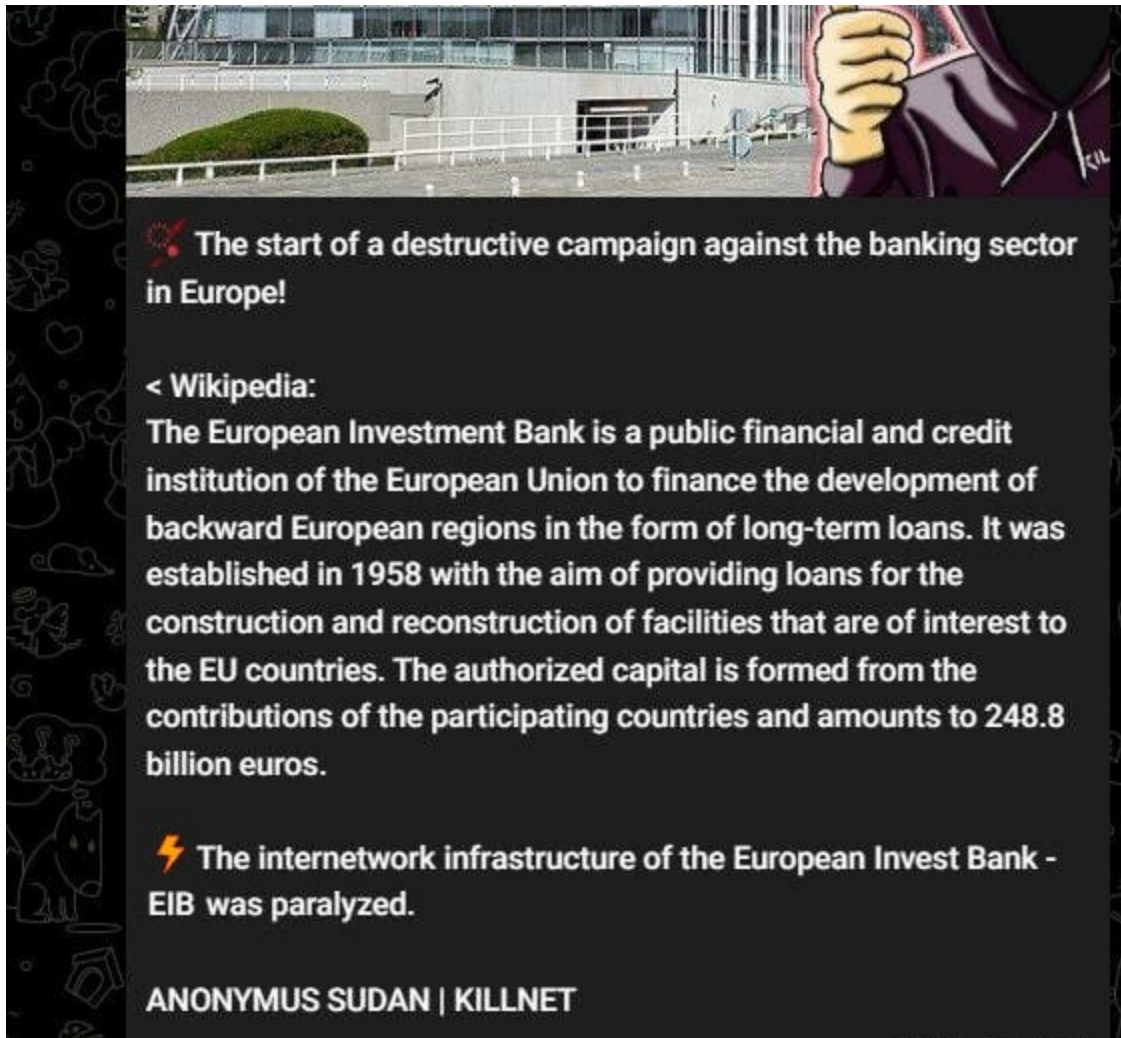
June 20, 2023

[Update] June 22, 2023: KillNet and Anonymous Sudan targeted the International Finance Corporation.

The **Darknet Parliament campaign** has officially begun with an attack on a European financial institution. The KillNet hackers have listed the **European Investment Bank (EIB)** as one of their targets. This marks the beginning of a series of anticipated future attacks.

On June 19, 2023, the hackers announced on their Telegram channel that they had “paralyzed” the inter-network infrastructure of the European Investment Bank. As the main shareholder in the European Investment Fund (EIF), the EIB provides funding to **SMEs** and serves as a state institution, providing loans for infrastructure projects in several European countries.





The start of a destructive campaign against the banking sector in Europe!

< Wikipedia:
 The European Investment Bank is a public financial and credit institution of the European Union to finance the development of backward European regions in the form of long-term loans. It was established in 1958 with the aim of providing loans for the construction and reconstruction of facilities that are of interest to the EU countries. The authorized capital is formed from the contributions of the participating countries and amounts to 248.8 billion euros.

⚡ The internet infrastructure of the European Invest Bank - EIB was paralyzed.

ANONYMUS SUDAN | KILLNET

Parliament attacks European Investment Bank

The European Investment Bank later confirmed the attack with a [Twitter post](#), stating that the availability of their website was affected.

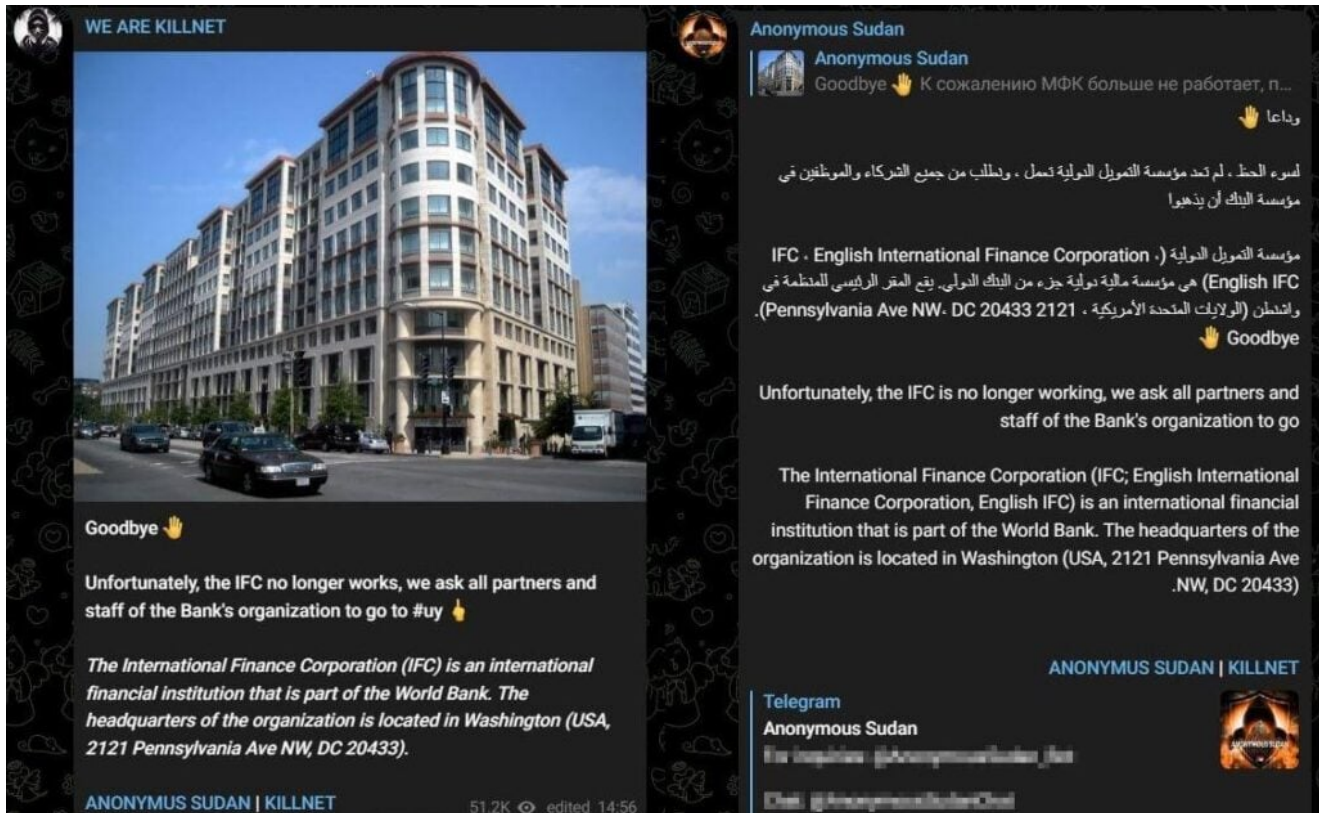


EIB's statement on Twitter

KillNet and Anonymous Sudan Disrupts International Finance Corporation's Website

KillNet announced on Telegram on June 21, 2023, that they had targeted the **International Finance Corporation (IFC)** website with Anonymous Sudan. The IFC is an international financial institution that is part of the World Bank.

KillNet stated in the post that the IFC website is no longer operational; Anonymous Sudan, the hacker group's parliamentary colleague, followed by forwarding KillNet's post on their own Telegram channel.



KillNet and Anonymous Sudan post about International Finance Corporation (IFC) on Telegram

How Did Hackers Establish the Darknet Parliament?

Darknet Parliament, the term introduced by the notorious hactivist group KillNet, has quickly gained traction, becoming the latest buzzword in the cyber media. KillNet introduced the phrase in a Telegram post **on June 16**.

In the post, they outlined a plan to attack **Europe's banking system**. They made the post in a government briefing report format, with their decisions and solutions numbered, such as **Decision No. 0191** and **Solution No. 0191**. This indicates a possible inclination towards institutionalization or a shift to a more stringent hierarchical structure.



WE ARE KILLNET



📢 72 hours ago, three heads of hacker groups from Russia and Sudan held a regular meeting in the parliament of the DARKNET, and came to a common decision:

⚡ DECISION No. 0191

- Today we are starting to impose sanctions on the European banking transfer systems SEPA, IBAN, WIRE, SWIFT, WISE.

Translation^

× 72 hours ago, three heads of hacker groups from Russia and Sudan held a regular meeting in the DARKNET parliament, and came to a common decision:

× SOLUTION No0191

- Today we are starting to impose sanctions on the European banking transfer systems SEPA, IBAN, WIRE, SWIFT, WISE.

WE ARE KILLNET 🤪

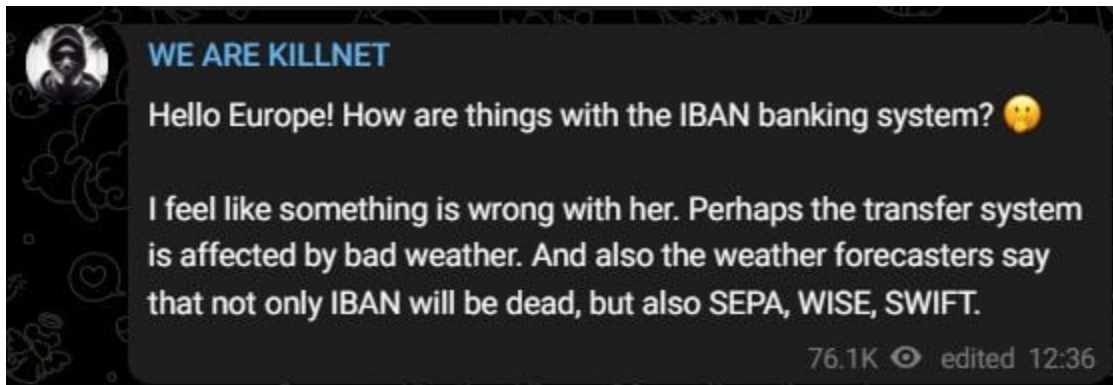
90.4K 👁 edited 13:56

KillNet's

post about the Darknet Parliament

According to KillNet's statement, the leaders of three hacker groups have agreed to "impose sanctions" on the targets. **European and US banks, SWIFT, and the US Federal Reserve System**, are among the targets. Financial targets mentioned in the warning also include **SEPA, IBAN, Wire** money transfer service, and **Wise**, a money transfer company.

KillNet's warning before posting the Darknet Parliament "pact" is shown below:



KillNet's

initial announcement before the Darknet Parliament post

Key Threat Actors in Darknet Parliament

Killnet, REvil, and Anonymous Sudan, three prominent **pro-Russian** threat actors, have joined forces for this campaign; although not confirmed, the Darknet Parliament campaign targeting European financial institutions could be orchestrated in response to **European support for Ukraine**.

Anonymous Sudan shared the Darknet Parliament message on its own Telegram channel to confirm the planned attacks. The Darknet Parliament's threat actors' polls, which are shared across their Telegram channels, showed **SWIFT as the first target** before EIB was hit on June 19.

UserSec hacker group has also forwarded the messages, suggesting they may be involved in planned attacks. The UserSec group has previously collaborated with Killnet and Anonymous Sudan.

KillNet Shifts Targets: What Is the Motive Behind the Darknet Parliament?

During the ongoing conflict between Ukraine and Russia, KillNet, a pro-Russian hacktivist group, has emerged as a significant cyber threat. Killnet actively engages in cyber warfare by launching DDoS attacks against countries that support Ukraine, with a particular emphasis on **NATO countries**.

Since its transformation into a hacktivist group in February 2022, Killnet has targeted various sectors and countries. Their attacks have impacted government organizations, ministries, as well as industries such as aviation, defense, and healthcare. The scope of their targets

extends to **European and Western countries**, including the US, UK, Germany, Italy, Romania, Lithuania, Estonia, and Poland.

Although they have carried out attacks against Ukraine, KillNet's focus extends beyond the conflict, as they actively support Russian geopolitical interests on a global scale. Their primary objective has been to disrupt web services and cause harm to their targets rather than pursue financial gain. Thus, the hacktivist group's recent focus on financial organizations suggests a **possible alignment** with their broader agenda.

The Darknet Parliament threat actors are most likely seeking vengeance by imposing their own sanctions on European financial organizations in response to the **sanctions imposed by Western financial institutions on Russia**. Western nations have been taking measures to restrict Russia's access to funds, such as freezing assets of Russia's central bank in their respective countries. Major Russian banks have also been excluded from the international financial messaging system SWIFT, resulting in delayed payments for **Russian oil and gas**.

Anonymous Sudan Joins the Darknet Parliament

KillNet-affiliated Anonymous Sudan, a politically and religiously motivated hacker group from Sudan, has been conducting DDoS attacks on various countries and critical infrastructure since January 23, 2023. Original Anonymous Sudan emerged in response to **political and economic challenges**, utilizing hacking and DDoS attacks for digital activism, highlighting government-imposed censorship and restrictions on free speech.

Notably, the group has shown persistent **support for Russian hacktivism**, emphasizing the reciprocal support between Sudanese and Russian hackers.

Unmasking the Role of REvil Ransomware

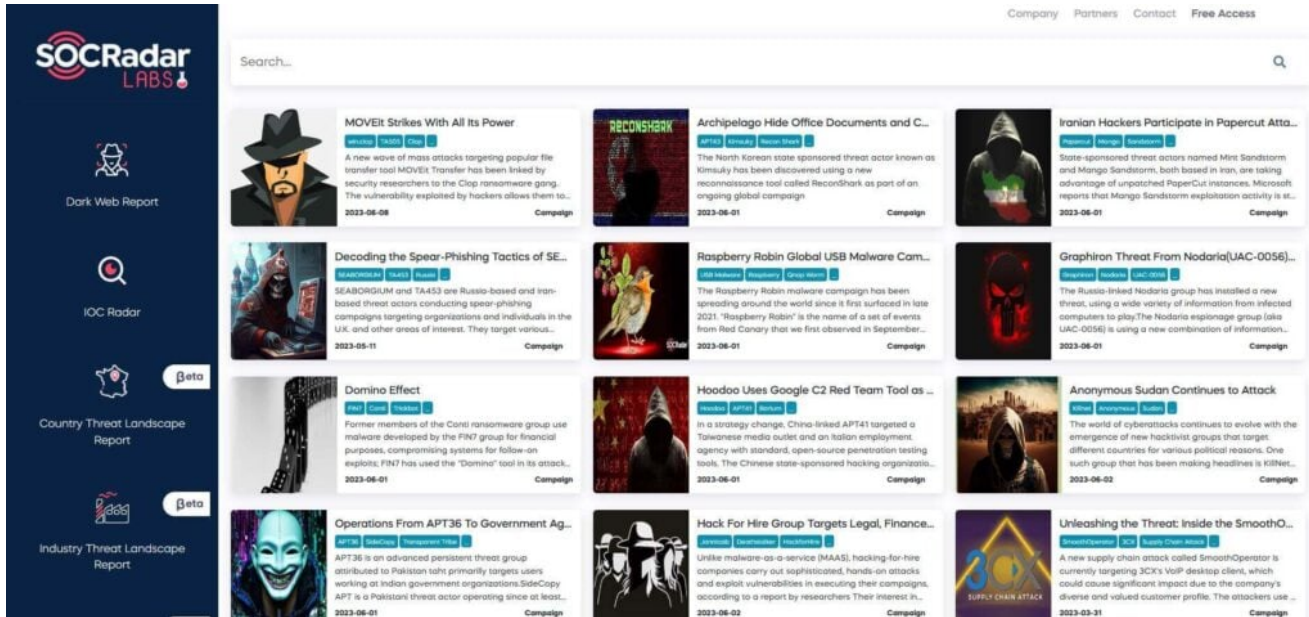
REvil, also known as **Sodinokibi**, is a highly active ransomware group driven by financial motives. Established in 2019 and believed to operate from Russia, REvil has gained notoriety for its involvement in prominent attacks, such as the Kaseya incident.

Vx-underground on Twitter has shared a video released by REvil, which sheds light on the collaboration between **REvil and KillNet** as they target the European banking system. In the video, REvil emphasizes they are "**sufficiently familiar**" with the European financial infrastructure.

<https://twitter.com/vxunderground/status/1669053086495563777>

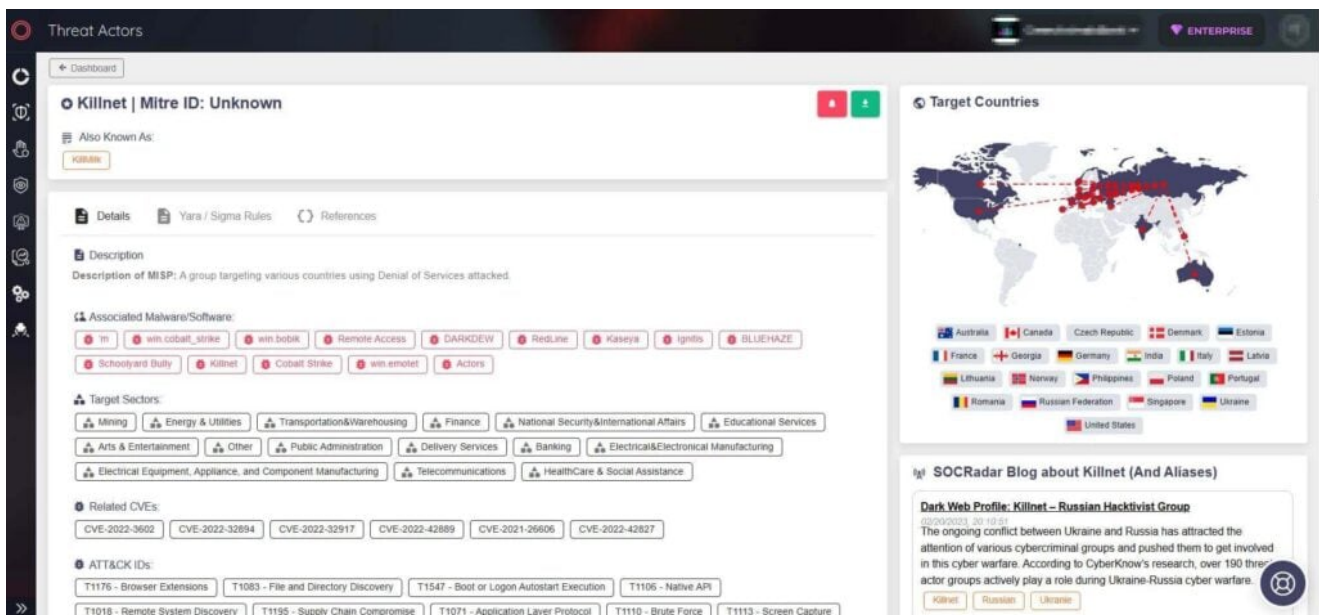
Discover the Latest Campaigns with SOCRadar

Discover the latest campaigns conducted by threat actors with diverse motivations by visiting SOCRadar's dedicated campaign page. The [SOCRadar Labs Campaigns](#) page provides up-to-date information on the latest campaigns carried out by threat actors, allowing you to track the timeline, associated threat actors, and indicators of compromise (IoC) for each campaign.



SOCRadar Labs Campaigns

With SOCRadar's [Threat Actor Tracking](#), organizations can effectively track and analyze the activities of threat actors, including KillNet, REvil, and Anonymous Sudan, engaged in the Darknet Parliament, among numerous other threats. SOCRadar's comprehensive platform provides real-time updates and actionable intelligence on all monitored threat actors, enabling proactive defense measures.



KillNet's Threat Actor Profile on SOCRadar



[Learn more >](#)

**DISCOVER YOUR
EXTERNAL ATTACK
SURFACE**