



| Flash |

German Protests Supported by Pro-Russian Threat Actor

F-2024-01-12a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, Supply Chains

January 12, 2024

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 9:30 AM (EST) on January 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash |

German Protests Supported by Pro-Russian Threat Actor

› Key Findings

- NoName057(16), a pro-Russian threat actor group that normally targets supporters of Ukraine, hacked German websites in a show of support for protesting farmers.
- The group is likely opportunistically supporting the farmer protests because elements of the movement may be in favor of reducing the level of aid provided to Ukraine.
- European Union (EU)-wide elections are scheduled for June 2024, and far-right politicians who oppose aid to Ukraine will likely perform well.
- These politically-motivated hacks are intended primarily to stoke underlying social tensions while creating an impression of wider fissures in EU society, mainly around the cost of living and immigration, and are a common tactic of pro-Russia and Russian-sponsored actors.

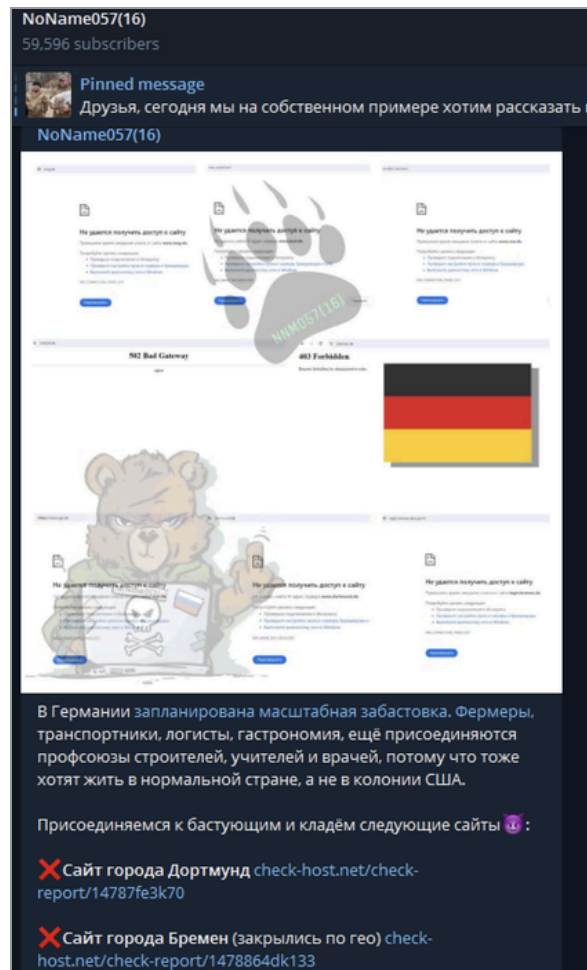
Details

On January 10, 2024, hacktivist threat actor group NoName057(16) claimed to have carried out attacks against multiple German websites, probably in an effort to stoke underlying social tensions while creating an impression of wider fissures in EU society. The attacks came ahead of the third day of nationwide protests by German farmers and truckers from January 8–15, 2024.

- Farmers are protesting against a late 2023 budget agreement by the German government that reduces farming subsidies and raises taxes on diesel.¹
- Farmers are staging protests across German cities using tractors to clog traffic, with a final protest in the capital of Berlin to be held on January 15. Farmers have been protesting since December 2023, and further protests are likely.²
- NoName057(16) targeted municipal websites of cities ahead of the farmer protest activity, including Dortmund and Bremen. NoName057(16) is likely opportunistically supporting the farmer protests hoping to assist elements of the movement that call for less aid in support of the Ukrainian war effort. However, the group has a history of claiming attacks that have little impact.

¹ [hXXps://www.marketplace\[.\]org/2024/01/09/germany-farmers-tractor-blockade/](https://www.marketplace.org/2024/01/09/germany-farmers-tractor-blockade/)

² [hXXps://www.bbc\[.\]com/news/world-europe-67911739](https://www.bbc[.]com/news/world-europe-67911739)



NoName057(16)'s claim of disrupting German websites

Source: ZeroFox Intelligence

Analyst Commentary

NoName057(16) is a pro-Russia hacktivist group that specializes in distributed denial-of-service (DDoS) attacks. During the Ukrainian counteroffensive of mid-2023, the group largely focused its attacks on supporters of Ukraine, targeting European websites and infrastructure facilities.

- One of NoName057(16)'s more notable campaigns occurred in mid-June, when the group conducted DDoS attacks against a number of Dutch port websites, including that of the port of Rotterdam, Europe's largest port. The group cited the

Dutch government's plan to buy and send tanks from Switzerland to Ukraine as the reason behind its attack.³

- The attack was one of the group's more successful, bringing down multiple websites for several hours and disrupting their ability to process some trade.
- ZeroFox also observed the entity targeting over 30 European government and logistics websites in Italy, Sweden, Greece, Germany, and Bulgaria.⁴ Port domains were the main sector targeted, indicating the group may have been attempting to cause logistics and supply chain disruptions.

While hacks in support of protesting farm workers appear to be a different *modus operandi*, it is more likely an evolution in tactics, as NoName057(16) likely remains focused on weakening Western support for Ukraine. At the onset of the farmer protests, EU authorities warned they were concerned far-right groups were infiltrating the protests.

- In some instances, this appears to be true. During a protest in the large southern city of Munich, members of the Europe-wide anti-immigration group Identitarian Movement (IB) participated in protests.⁵ While these groups make up the fringe of the farmer protests, they have on occasion outnumbered farm workers at protests and staged some of the most destructive protest activity.

Since Russia's war against Ukraine broke out in February 2022, far-right politicians (and those that oppose support for Ukraine) have secured notable electoral wins in Italy, the Netherlands, Finland, Denmark, Sweden, Slovakia, and Hungary.⁶

- With the exception of Slovakia, where the winning presidential candidate openly campaigned on ending support for Ukraine,⁷ these politicians have primarily campaigned on limiting immigration and the cost of living, occasionally linking less support for Ukraine as key to bringing down inflation.
- However, their victories have coincided with less financial and military support for Ukraine, with the EU currently struggling to pass a 2024 aid package to Ukraine.

³ [hXXps://nltimes\[.\]nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks](https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks)

⁴ ZeroFox Intelligence

⁵ [hXXps://euobserver\[.\]com/opinion/157900](https://euobserver[.]com/opinion/157900)

⁶

[hXXps://www.reuters\[.\]com/world/europe/far-right-parties-eye-gains-next-years-eu-parliament-elections-2023-12-03/](https://www.reuters[.]com/world/europe/far-right-parties-eye-gains-next-years-eu-parliament-elections-2023-12-03/)

⁷ [hXXps://www.politico\[.\]eu/article/slovakia-new-prime-minister-robert-fico-ukraine-war/](https://www.politico[.]eu/article/slovakia-new-prime-minister-robert-fico-ukraine-war/)

Conclusion

Campaigns conducted by NoName057(16) are very likely to continue to be disruptive in the short term but have limited medium to long-term impact. The group very likely lacks the capability to significantly disrupt operations in Germany or sow widespread discord amongst its electorate.

However, ZeroFox anticipates activity by pro-Russia groups will likely escalate ahead of the elections. Threat actors such as NoName057(16) likely view successful anti-government protests in countries that support Ukraine, like Germany, as key to reducing Western support for Ukraine. EU-wide elections are scheduled for June 2024, and incumbent EU authorities are concerned that far-right politicians less supportive of Ukraine will gain further ground. However, EU-wide economic conditions like inflation deceleration and the slowing of immigration will have the biggest influence on whether far-right politicians who oppose aid to Ukraine will be successful.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
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.	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.
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.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
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.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%