



WHISTLEBLOWER DOCUMENTS DISCLOSE RUSSIAN GOVERNMENT CYBERWARFARE TACTICS

ZEROFOX INTELLIGENCE

F-2023-04-03a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Sensitive Information Disclosures, Threats to
Critical Infrastructure, Government

April 3, 2023



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 (DST) on April 3, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Whistleblower Documents Disclose Russian Government Cyberwarfare Tactics

Key Findings

- A Russian government subcontractor employee has leaked thousands of documents detailing Russia's cyberwarfare capabilities.
- The leaked files, now called the Vulkan Files, have drawn comparisons to the immensity and importance of the documents leaked by Edward Snowden in the United States in 2013.
- These files demonstrate the Russian government's focus on its cyberwarfare capabilities and its multilayered approach to advancing these capabilities.
- The Vulkan Files likely diminish the ability of the Russian government to utilize plausible deniability to distance itself from cyber actions that have taken place in parallel with its military actions.

Analyst Commentary

An unnamed whistleblower has provided nearly a dozen European and American media outlets with thousands of documents from a Russian government subcontractor named Vulkan.¹ The whistleblower, who indicated that they were disillusioned by Russia's war in Ukraine, began providing the documents to the media outlets shortly after Russia's invasion of Ukraine in February 2022. Since that time, the various media outlets—which include the United States' *Washington Post*, Germany's *Der Spiegel*, the United Kingdom's *The Guardian*, and France's *Le Monde*—have worked together to

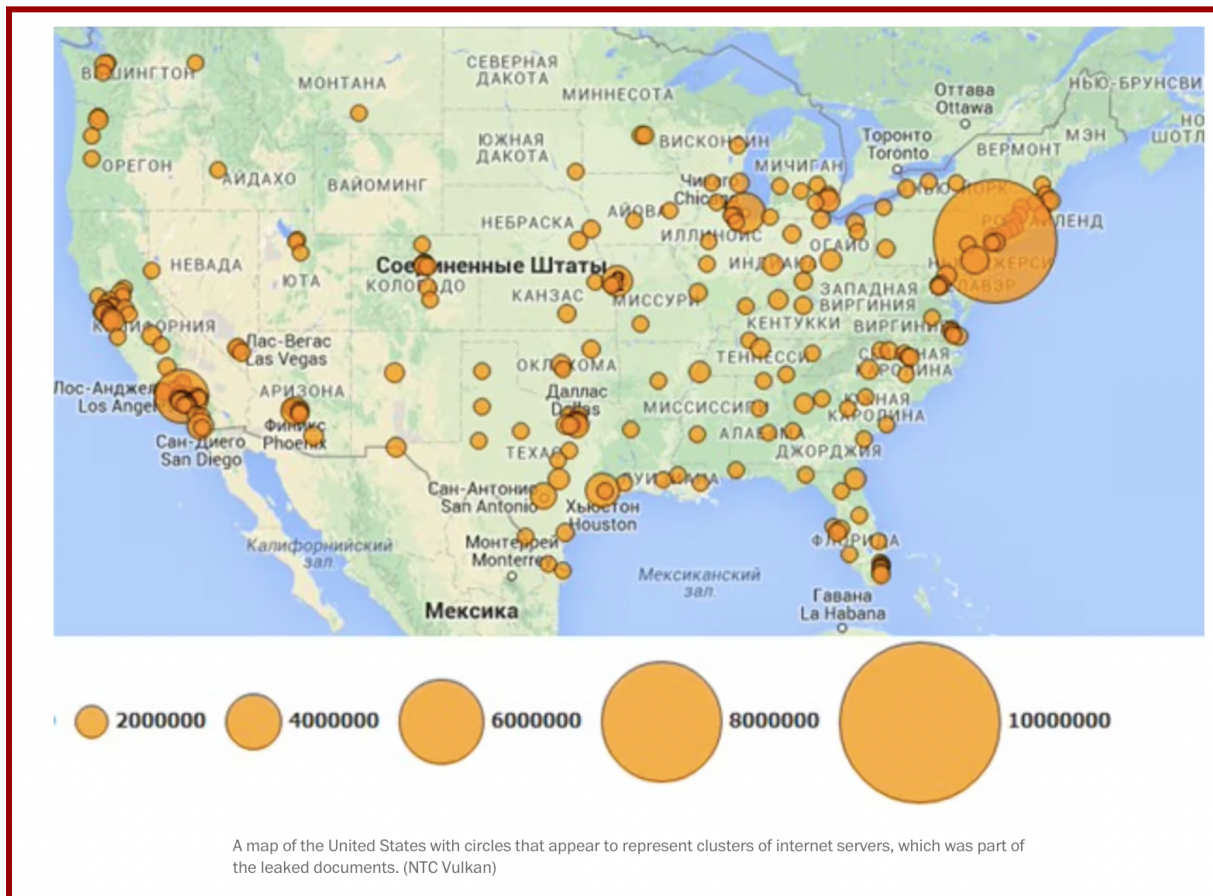
1

[hXXps://www.theguardian\[.\]com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics](https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics)



analyze invoices, emails, and projects that Vulkan has been engaged with since 2016 and draw conclusions about the Russian government's cyberwarfare capabilities.²³

The files indicate the Russian government has contracted for a multilayered approach to cyberwarfare. This includes utilizing Vulkan's technology to map out the internet to identify vulnerabilities to be cataloged for possible exploitation later, monitoring and surveilling certain parts of the internet, and creating fraudulent social media accounts in order to spread propaganda around various topics.⁴



U.S. Map Showing Clusters of Internet Servers

Source:

[hXXps://www.washingtonpost\[.\]com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/](https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/)

² [hXXps://www.theregister\[.\]com/2023/03/31/vulkan_files_russia/](https://www.theregister.com/2023/03/31/vulkan_files_russia/)

³

[hXXps://www.lemonde\[.\]fr/en/pixels/article/2023/03/30/inside-vulkan-the-digital-weapons-factory-of-russian-intelligence-services_6021230_13.html](https://www.lemonde.fr/en/pixels/article/2023/03/30/inside-vulkan-the-digital-weapons-factory-of-russian-intelligence-services_6021230_13.html)

⁴

[hXXps://www.washingtonpost\[.\]com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/](https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/)

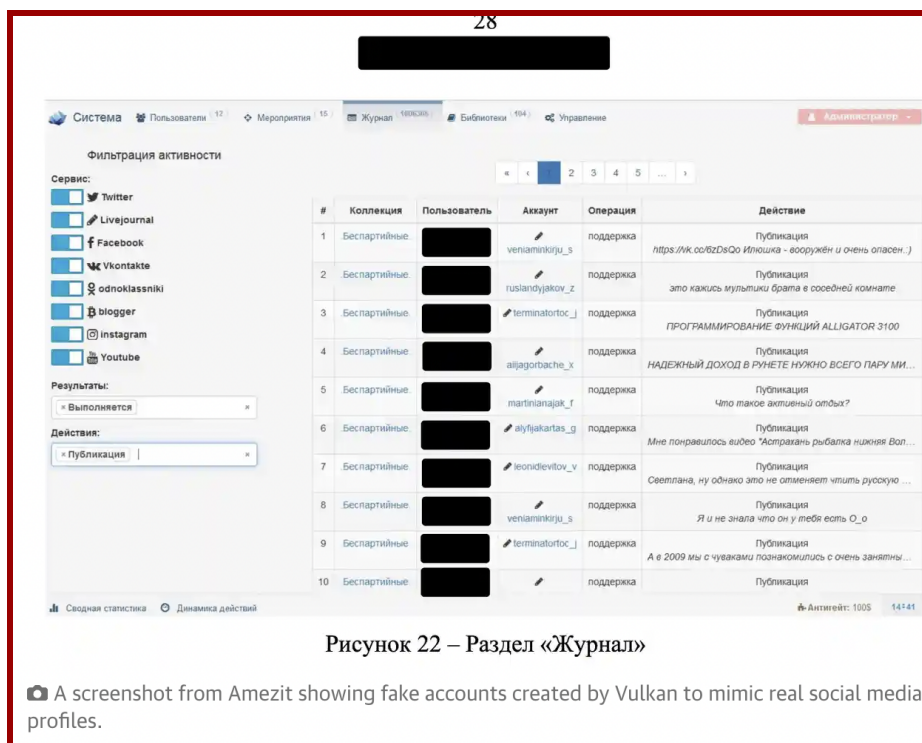


Рисунок 22 – Раздел «Журнал»

A screenshot from Amezit showing fake accounts created by Vulkan to mimic real social media profiles.

Fake Accounts Created by Vulkan to Mimic Real Social Media Profiles

Source:

[hXXps://www.theguardian\[.\]com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics](https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics)

The leaked documents offer a rare glimpse into the depth and breadth of the cyberwarfare tactics that the Russian government has strategically focused on over the last decade and demonstrate the lengths to which Russia will go to obtain such tools to have at its disposal. This exposure has drawn comparisons to the 2013 leaks by U.S. National Security Agency contractor Edward Snowden, which included thousands of documents detailing surveillance being conducted throughout the world.⁵

Despite suspicions to the contrary, the Russian government had thus far been able to maintain plausible deniability regarding cybercriminals advancing foreign policy goals through cyberattacks that were in support of the state but not directly linked to the government. However, the findings from the Vulkan Files likely demonstrate that there are direct links between the cybercriminals' actions and the Russian government, as Vulkan has been tied to both Russian security services and Sandworm—the Russian military hacking group accused of launching the NotPetya malware.⁶ As shown below,

⁵

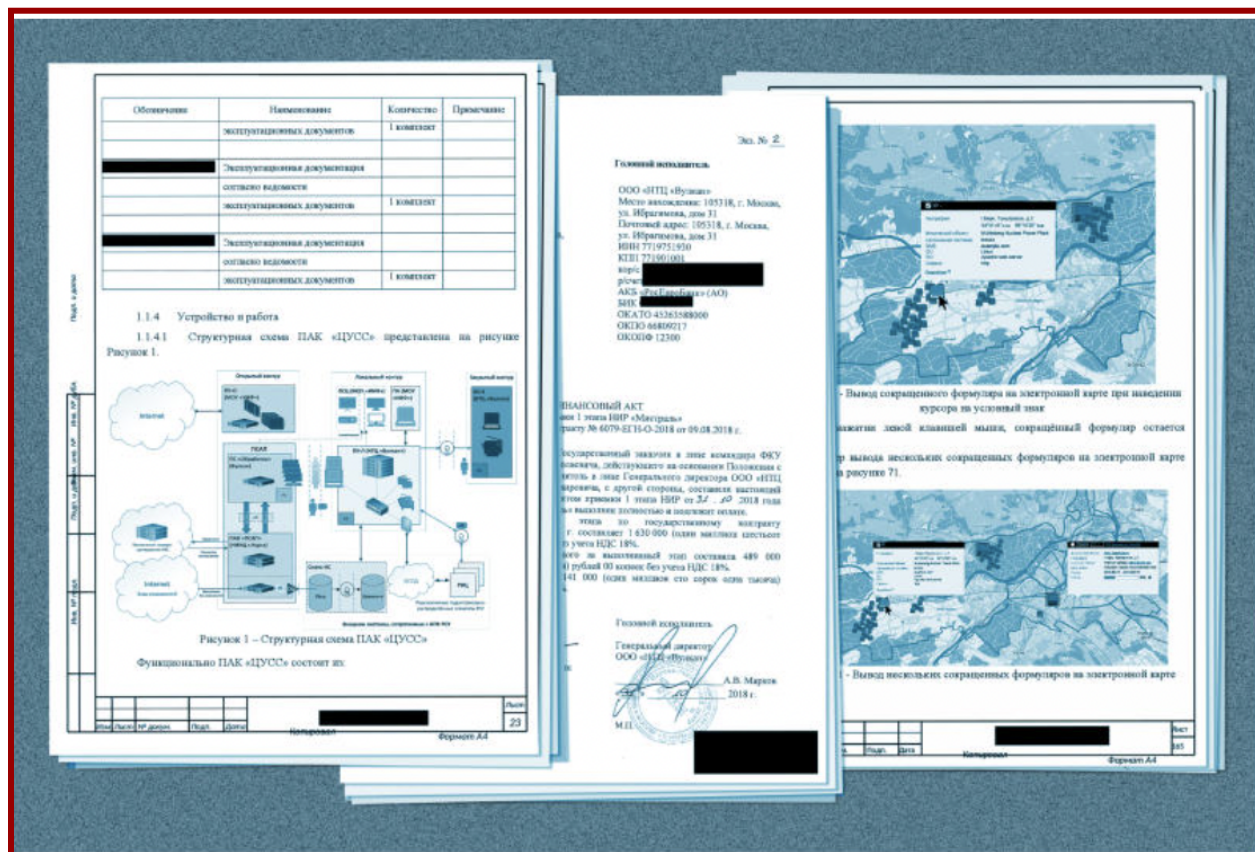
[hXXps://www.theguardian\[.\]com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded](https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded)

⁶

[hXXps://www.spiegel\[.\]de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236](https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236)



these leaked files demonstrate the measures that the Russian government has taken not only to monitor and surveil the internet where possible and engage in offensive attacks but also to manipulate the internet in its favor.



Vulcan Documents Explaining Functioning of Tools Offered to Russian Security Services

Source:

https://www.lemonde.fr/en/pixels/article/2023/03/30/vulkan-files-what-russian-company-s-internal-documents-reveal-about-kremlin-s-cyberwarfare-obsession_6021238_13.html



Appendix: 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.