

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

A pro-Russian hacker group named Zarya is building Mirai variants to grow its DDoS botnet used to perform attacks on the west. Akur group provides bulletproof hosting services for pro-Russian hackers. Zarya is hosting its propaganda website, attack campaign log, and malware on hosts in the akur[.]group domain.

The new malware and cooperation between Zarya and Akur group demonstrate how pro-Russian hackers are growing their tactics, techniques, and procedures (TTPs) as the Russo-Ukrainian conflict enters its second year. Pro-Russian hackers have moved beyond the basic denial-of-service scripts and crowdsourced attacks to more advanced and potent techniques, leveraging and cooperating with other hacker groups within the Russian-speaking community.

Background

The ongoing Russo-Ukrainian conflict has resulted in a rising number of cyber-attacks, with Russia and Ukraine primarily leveraging Denial-of-Service attacks to degrade and disrupt their adversary's network and applications. From government websites to critical infrastructure systems, no target has been immune to these attacks.

As the conflict continues to escalate, the digital threat actors involved have become more organized and sophisticated, with the emergence of social communities supporting malicious activities through various platforms like online forums and social media groups. This has resulted in a proliferation of malicious activities and the spread of sophisticated tools and techniques across the internet, sometimes even supporting criminal activities such as buying and selling stolen data or hosting malware used in cyber-attacks.

ZARYA

Zarya, also referred to by its Russian name Заря, which translates to "dawn," is a pro-Russian hacker group that emerged in March 2022. Initially, the group operated as a special forces unit under the command of Killnet. The group's objectives and motivations shifted as the conflict in Ukraine evolved. This led to a breakaway from Killnet, with the group at times going by 0x000000, and a focus on recruiting skilled hackers from other pro-Russian threat groups that were burning out in the spring of 2022.

In May 2022, Zarya rejoined Killnet as part of a larger project called ЛЕГИОН, also known as its translation, 'Legion.' During the summer of 2022, the group, Zarya Legion, established itself as a leading force within Legion, setting an example for other groups and eventually becoming an independent entity known as just Zarya in August 2022.


The group is primarily known for its involvement in Denial-of-Service attacks, website defacement campaigns, and data leaks. These tactics have been leveraged to support the group's pro-Russian agenda and have significantly disrupted targeted organizations and individuals.

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group


February 20, 2023


KILLNET

 **KillNet**

Наша активность началась ещё в рядах KillNet, когда четкого разделения на умения не было, у всех была только одна цель и четкая концентрация на ней. В основном мы вычисляли слабые места для DDoS'a и координировали будущие атаки. Не сказать, что мы были созданы для этой работы и нам нравилось, но справлялись мы достаточно неплохо. Однако, нам хотелось большего, нам хотелось взламывать цели, а не просто тормозить их работу


Март 2022


 **0x000000**



В итоге мы добились своего, доказав, что способны на большее, чем на просто вычисление слабых мест и поиск бекенда. Тогда и был создан первый, отдельный чат, куда шёл набор людей извне. Людей мы набирали тайно: забирали лучших бойцов из чужих уже "погибших" команд, своих знакомых, в старых чатах и всех, с кем мы работали раньше. Таким образом, нам удалось организовать целую структуру внутри киллнета, состоящую из одних хакеров


Апрель 2022


 **Заря Легион**



Вскоре появился Легион, дочерний проект KillNet. А наш чат с проверенными временем ребятами тем временем перерос в полноценную команду. Было решено организовать переход команды в Легион, из-за чего мы по праву считаемся самым старым его объединением. После перехода мы начали открытый набор людей, проверяя каждого отдельно и ведя свою собственную внутреннюю политику

Май 2022

 **Заря**



Мы продолжали расти дальше, переформатировав старый канал KillNet'a с "народным движением" в свой собственный, дав тем самым пример другим группам Легиона, которые начали копировать наше поведение. Спустя некоторое время, канал вырос, а нас начали воспринимать как отдельную команду. И тогда мы поняли, что наше ведение информационной войны сильно разнится и мы приобрели статус "независимых", пополнив ряды пророссийских группировок

Август 2022

Figure 1: Zarya history

AKUR GROUP

The Akur Group is a pro-Russian threat group formed in November 2022. Despite having a small number of subscribers, fewer than one hundred, the group has made its presence known in the pro-Russian hacktivist community. In recent months, the group has been observed launching Denial-of-Service attacks and website defacement campaigns.

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

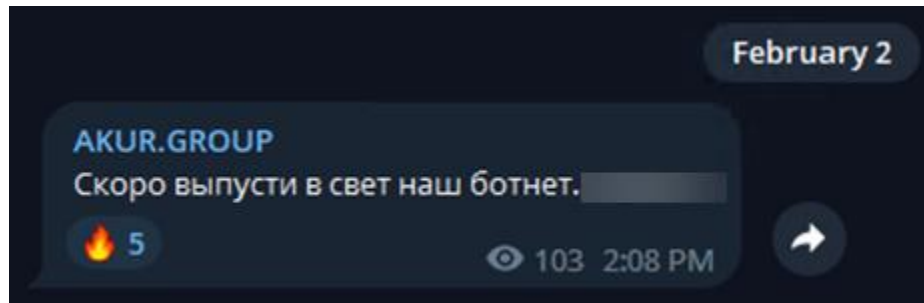


Figure 2: Akur referencing its new botnet

Additionally, the Akur Group has been attempting to establish itself as a hosting service for other pro-Russian hacker groups. The group registered its domain, akur.group, in November 2022 through Reg.ru and leveraged Cloudflare to secure its website.

Cyberfront

The Akur Group is currently providing hosting services for the website of the pro-Russian hacker group Zarya. This website, known as 'Zarya - CyberFront,' serves as a platform for the group to showcase its recent hacking activities, data leaks, and other relevant information. The CyberFront website provides insight into the group's tactics, targets, and objectives and serves as a means of communication with its supporters and potential recruits.

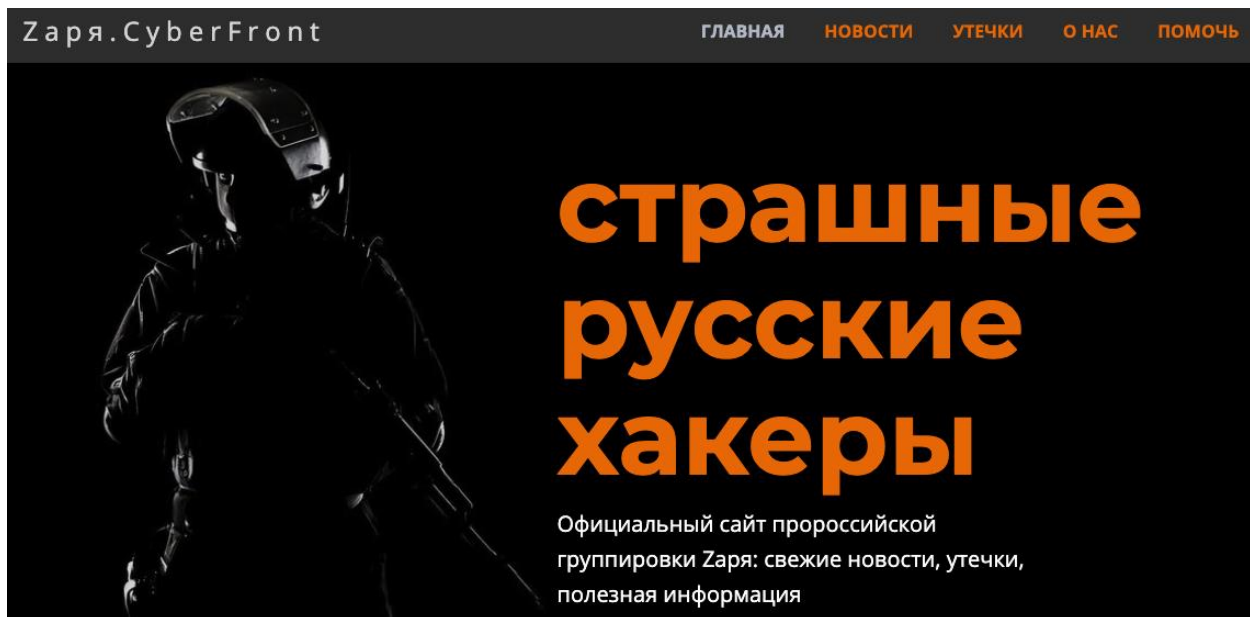


Figure 3: Zarya CyberFront website hosted on Akur Group (<https://zarya.jakur.group/>)

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

Zarya's CyberFront website provides information about targeted verticals for the pro-Russian hacktivist group, Zarya. According to the website, the group primarily targets government agencies, service providers, critical infrastructure, and civil service employees.

LEAKS

On its Zarya's CyberFront website, the pro-Russian hacktivist group posts information about previous hacking campaigns, including leaked data. The website allows visitors to download leaked information, spreading the impact of the group's campaigns.

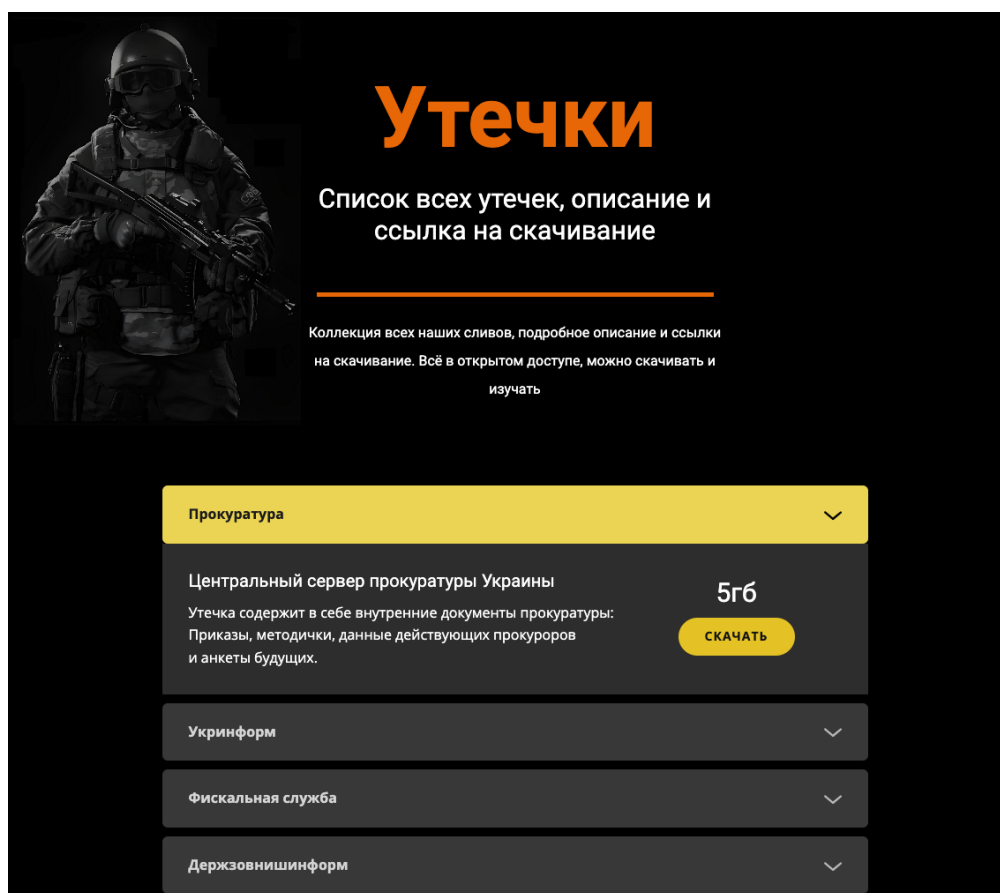


Figure 4: Zarya's hacking exploits and leaks page

Zarya's CyberFront website currently features links to 48 different hacking campaigns carried out by the group, along with the corresponding leaked data. Allegedly 655 Gigabytes worth of data. This information provides a comprehensive overview of the group's activities and highlights the significant impact of its campaigns and targeted verticals.

Radware Cybersecurity Advisory

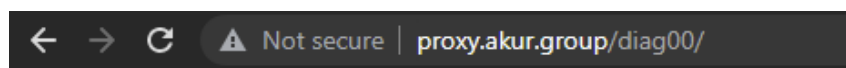
Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

MIRAI VARIANT

On February 12th, a compromised server in Vietnam attempted to exploit one of Radware's honeypots through a vulnerability known as [CVE-2016-20016](#). This vulnerability, a remote command execution flaw in MVPower CCTV DVR models, is commonly referred to as the JAWS webservice RCE.

The threat actors behind this attack attempted to deploy a shell script, which was meant to infect the deception device with a payload hosted on akur.group.



Index of /diag00

- [Parent Directory](#)
- [log21.arc](#)
- [log21.arm](#)
- [log21.armv5](#)
- [log21.armv6](#)
- [log21.armv7](#)
- [log21.i486](#)
- [log21.i686](#)
- [log21.m68k](#)
- [log21.mips](#)
- [log21.mips64](#)
- [log21.mpsl](#)
- [log21.ppc](#)
- [log21.sh4](#)
- [log21.spc](#)
- [log21.x86](#)
- [log21.x86_64](#)

Figure 5: List of malware binaries hosted on akur.group

The malware discovered on the website of the Akur Group is a variation of the well-known Mirai malware. Mirai, whose source code was published in 2016, is a type of malware that targets Internet of Things (IoT) devices, such as smart home appliances, internet-connected cameras, and, in some cases, cloud environments, to form a network of infected devices. The Mirai botnet is particularly dangerous because it can conduct large-scale Distributed Denial-of-Service (DDoS) attacks, where a massive amount of traffic is directed toward a single target, overwhelming the target's servers, and causing it to become unavailable to users.

One of the key features of this variant is its ability to conduct ten different types of DDoS attacks. In addition to its DDoS capabilities, this variant also features 11 exploits used for its propagation.

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

Reasons for Concern

This infection is significant because it shows that pro-Russian hacktivists are developing their tactics, techniques, and procedures (TTPs) as the Russo-Ukrainian conflict enters its second year. They have moved beyond basic denial-of-service scripts and crowdsourced attacks to more advanced and potent techniques.

Resources

[Interview](#) with Hesh, the founder of the Zarya hacker group.

Attack Methods

UDP FLOODS

- UDP Plain
- nUDP
- STDHEX

TCP FLOODS

- TCP-Stomp
- TCP-ACK
- TCP-SYN
- TCP-SYNdata
- TCP-Null
- TCP-Sack2

HTTP FLOODS

- App HTTP

EXPLOITS

- [Vacron RCE](#)
- [CCTV/DVR RCE](#)
- [Netgear setup.cgi RCE](#)
- [Eir D1000 WAN Side Injection](#)
- [D-Link UPnP SOAP](#)
- [CVE-2014-8361](#)
- [CVE-2015-2051](#)
- [CVE-2016-6277](#)
- [CVE-2016-20016](#)
- [CVE-2018-10561](#) / [CVE-2018-10562](#)
- [CVE-2018-17215](#)

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

Indicators of Compromise (IOC)

ZARYA WEBSITES

- `hxtps://zarya.akur[.]group/`

LOADER

- `113.30.191[.]198`
- `proxy.akur[.]group/diag00/`

BINARY HASHES

- `09cbbd696e50e03602de58aa62211f282675be9795b8b7f0134f6146241f6e7a`
- `33c816efd9bbe9d87edf15abaf761ad810dbc64faea8d5428bb696b719d8dca9`
- `0696ca672964b29f97127307671ba25d7e498cf00e3c4029d37ff7c2483b3002`
- `389b68a6a49e646e2c73f26ba02f5e9e490e80c0f48bcc79d2ae731b8c3bfe69`
- `6749dbab7e15bd56c86f2bc06ebe24405021fdc4446165011632293904fd256f`
- `6ff4c0ab17979b860cfb5cba854a5243095c70258077389bf0fd98c649ecd8c0`
- `a1d25afc015cca35c782246de5259805bbfe5d5943505e52ef945eedc160298f`
- `2898ef41e5939775ab204e0f3433b9d4659f75ffb59dba3fe71302037016a3f4`
- `a3bd1189420a005f6efafe3ed05ed4187be07b05436e23bb6491f9cb4d06ee86`
- `df514233cec90ff921b3d3599244c0a077e7724e6e13af8603185b17e5c27367`
- `348a34ca2fac56f68548b9041e618e81dd5460eafba31c054476e3e473ce3c31`
- `c79e9402894c8995dabb4278ed99adc941fca2cd72820c10a111d3ad6a049210`
- `931dc9c6a90b90f622adac475ef14aed302edd09079d0e0f11b820b1e27fa864`
- `e892f2e92635f30a7329926d07df05160664f6667e5731cccdf5fb30690b50c9`
- `3ad3113c6cd2bb83ca386bf997e28728768982e3d1f176bcfd788781270a0675`

BINARY SAMPLES

<https://bazaar.abuse.ch/browse/tag/Akur%20Group/>

Radware Cybersecurity Advisory

Pro-Russian Hacktivists Leverage Mirai Botnets Zarya Cyberfront & the Akur Group

February 20, 2023

EFFECTIVE DDoS PROTECTION ESSENTIALS

Hybrid DDoS Protection - On-premise and [cloud DDoS protection](#) for real-time [DDoS attack prevention](#) that also addresses high volume attacks and protects from pipe saturation

Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation - Promptly protect from unknown threats and zero-day attacks

A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors - High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers.

For further [network and application protection](#) measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate - using negative and positive security models for maximum accuracy

Auto policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's [Security Research Center](#). Additionally, visit Radware's [Quarterly DDoS & Application Threat Analysis Center](#) for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.