Is RuskiNet the Next Big Russian Hacktivist Group

By Orlaith Traynor

Published: 2025-10-30 · Archived: 2026-04-10 02:01:32 UTC

Emerging from pro-Russian cyber ecosystems, RuskiNet is the next rising hacktivist group.

A blend of cybercrime and a challenge to national security and public trust, RuskiNet uses hacktivism to push Russian agendas against adversarial nations.

Their attacks focus on phishing and malware attacks to gain access, relying on social engineering to gain a foothold in systems.

Let‘s dive into RuskiNet‘s threat intelligence profile, how to identify a potential breach, and what you need to consider in your mitigation efforts.

What is RuskiNet?

RuskiNet is a hacktivist group first observed in February 2025 via an X post. The gang is believed to be associated with Russian cyber operations; however, their attacks are launched from Eastern Europe.

Currently, public information about RuskiNet is limited, and some analysts question the credibility of the reported data leaks on dark web forums.

While RuskiNet is not officially state-sponsored by Russia, the hackers operate in ideological support of Russian geopolitical interests—such as targeting Ukraine, Israel, and nations in support of NATO.

Is RuskiNet an APT group?

Advanced Persistent Threat (APT) groups are typically state-sponsored cybercriminals who perform long-term espionage to compromise targets.

RuskiNet hasn‘t yet been confirmed as an APT group by threat analysts, as the group operates more akin to a hacktivist collective than an extended arm of Russia‘s GRU units.

With that being said, the group does align with similar goals to APTs like APT28 (Fancy Bear) or APT29 (Cozy Bear).

Notable cyberattacks (2025)

RuskiNet has utilized cyberattacks to disrupt critical infrastructure across the globe.

Since the beginning of 2025, RuskiNet has launched attacks against the US, Canada, Turkey, Israel, the UK, and India. Hackers targeted energy suppliers and shipping organizations with coordinated DDoS attacks to bring down daily operations and cause chaos.

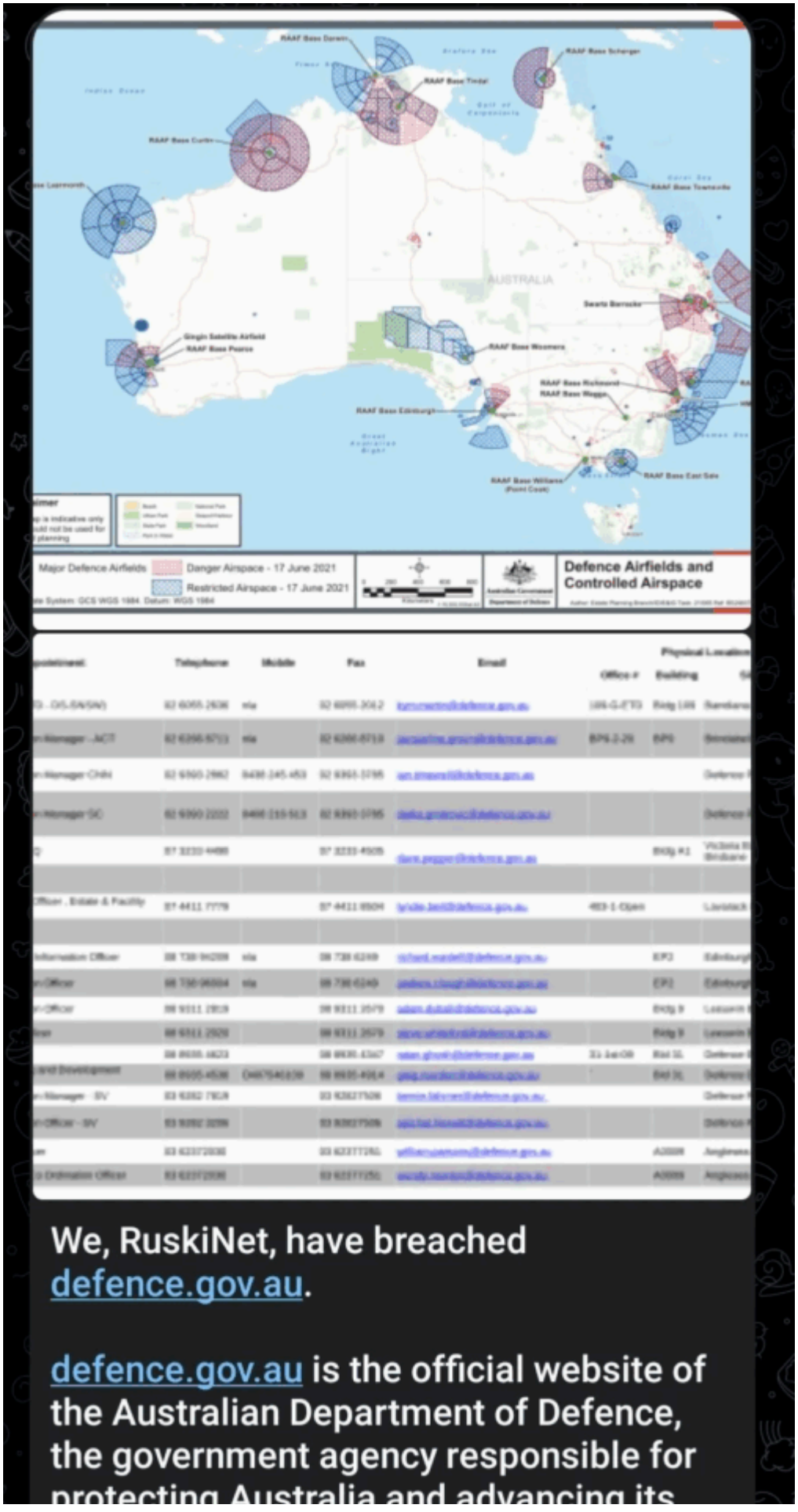
Here are some of their notable breaches since the group‘s inception at the beginning of 2025.

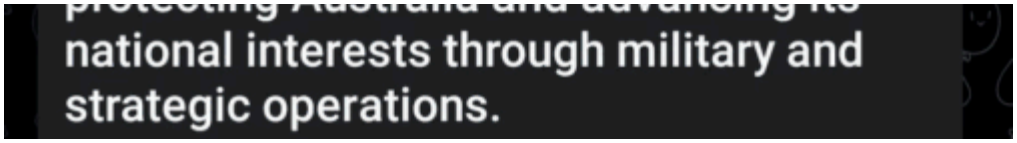
1. Targeted data breaches

On August 4, 2025, RuskiNet claimed responsibility for a targeted data breach on the Israeli intelligence team Mossad. The leak included identifiable data, including picture IDs, names, and email addresses.

An X post claiming RuskiNet‘s responsibility for the data breach on Mossad.

RuskiNet‘s geopolitical ambitions also led them to hack several Israeli critical infrastructure companies, including Enlight Renewable Energy, Tadiran New Energy, Electis, and Infinity Pack.


RAAF Base Darwin
RAAF Base Tindal
RAAF Base Scherger
RAAF Base Curtin
RAAF Base Townsville
AUSTRALIA
Swanbourne Barracks
Gingin Satellite Airfield
RAAF Base Pearce
RAAF Base Woomera
RAAF Base Richmond
RAAF Base Wagga
RAAF Base Edinburgh
RAAF Base Williamtown (Point Cook)
RAAF Base East Sale
Major Defence Airfields
Danger Airspace - 17 June 2021
Restricted Airspace - 17 June 2021
Defence Airfields and Controlled Airspace
We, RuskiNet, have breached defence.gov.au.
defence.gov.au is the official website of the Australian Department of Defence, the government agency responsible for protecting Australia and advancing its



A screenshot from RuskiNet's Telegram group detailing an alleged attack on the Australian Department of Defence. Source: CyberKnow on X

An X post detailing the RuskiNet cyberattack on an Israeli energy company.

Similarly, in Australia, the hacktivist group claimed to have breached the Australian Defence Force (ADF) site during operation "OpAustralia". However, cybersecurity analysts found that all the data revealed in the breach originated from publicly available sources, such as airfield reports and parliamentary reports. In this case, the intent was to cause disruption and chaos.

Current reporting suggests that not all released data may be legitimate, yet with the group's alleged connection to Russia, prevention and proper cyber defenses are key.

2. DDoS attacks

According to claims, RuskiNet hackers have targeted 16 industry sectors with DDoS attacks. Threat actors often use methods like VPNs, proxies, or TOR to conceal their real IP addresses and evade attribution.

In March 2025, the hacktivist group went after Colombia's energy sector, targeting Colombia Oil and Gas corporations in a coordinated DDoS attack. The digital operations were disrupted, but energy services continued undisrupted.

The cyberattack aimed to paralyze operations and send political messages rather than steal information. Especially since Colombia publicly showed Ukraine support at the UN General Assembly right before the attack.

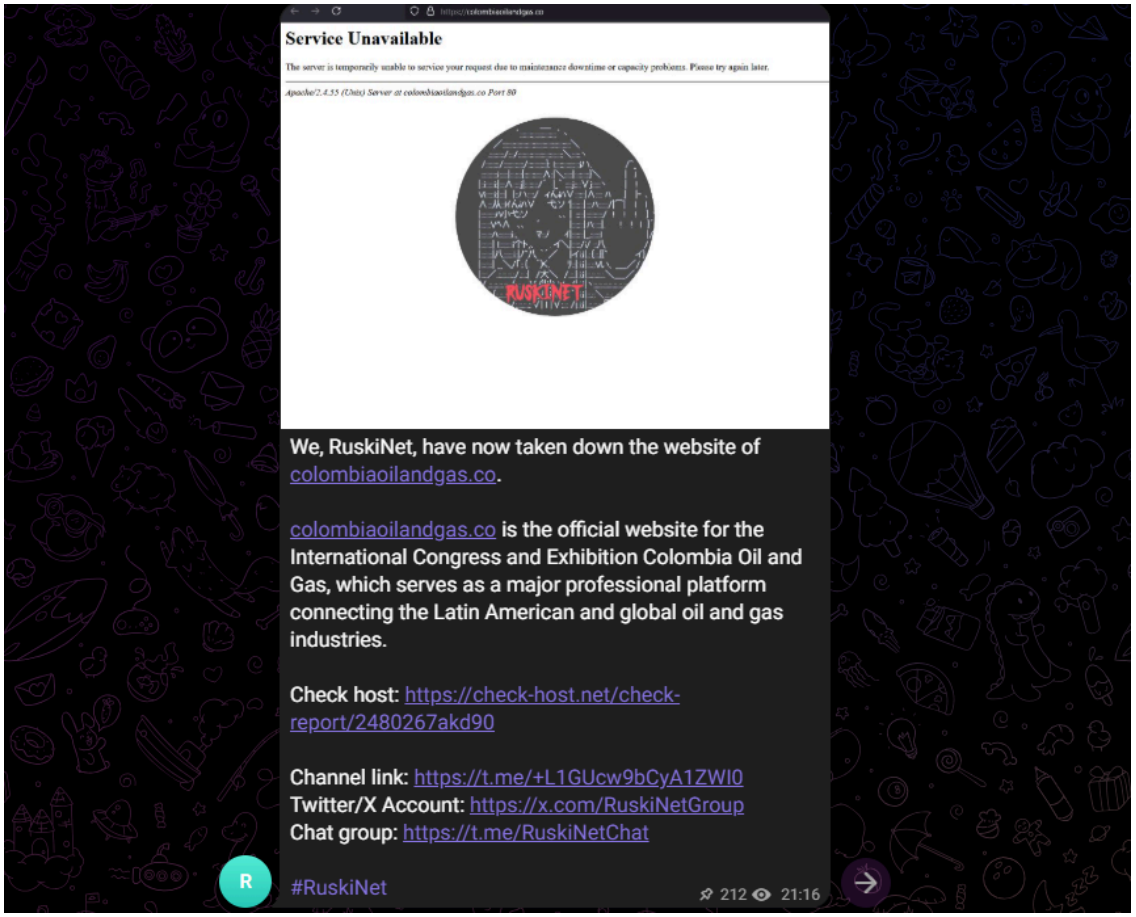


Figure 2. A screenshot from RuskiNet's Telegram channel claiming responsibility for the attack on Colombia Oil & Gas. Source: TechOwlShield

RuskiNet uses DDoS attacks frequently to deface websites and cause daily operations to grind to a halt.

3. Botnets

It's believed that RuskiNet utilizes botnets to perpetrate DDoS attacks and malware distribution. Earlier this year, around 13,000 compromised MikroTik routers were believed to be used by Russian state-sponsored hackers. The routers act as proxies, forwarding traffic without verifying its origin, helping attackers obfuscate detection.

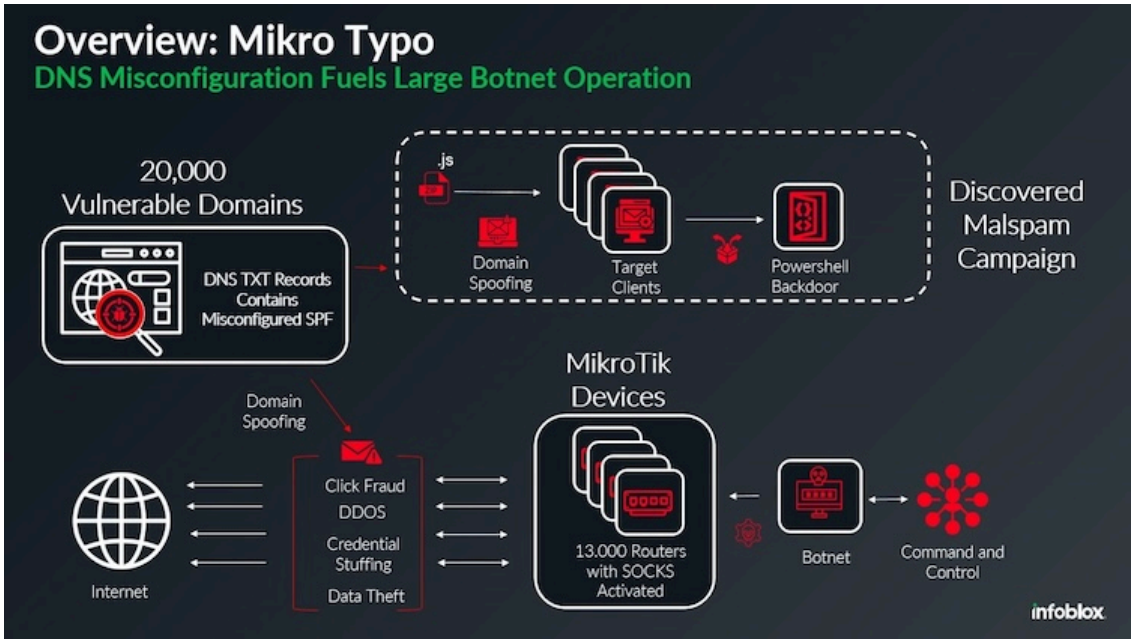


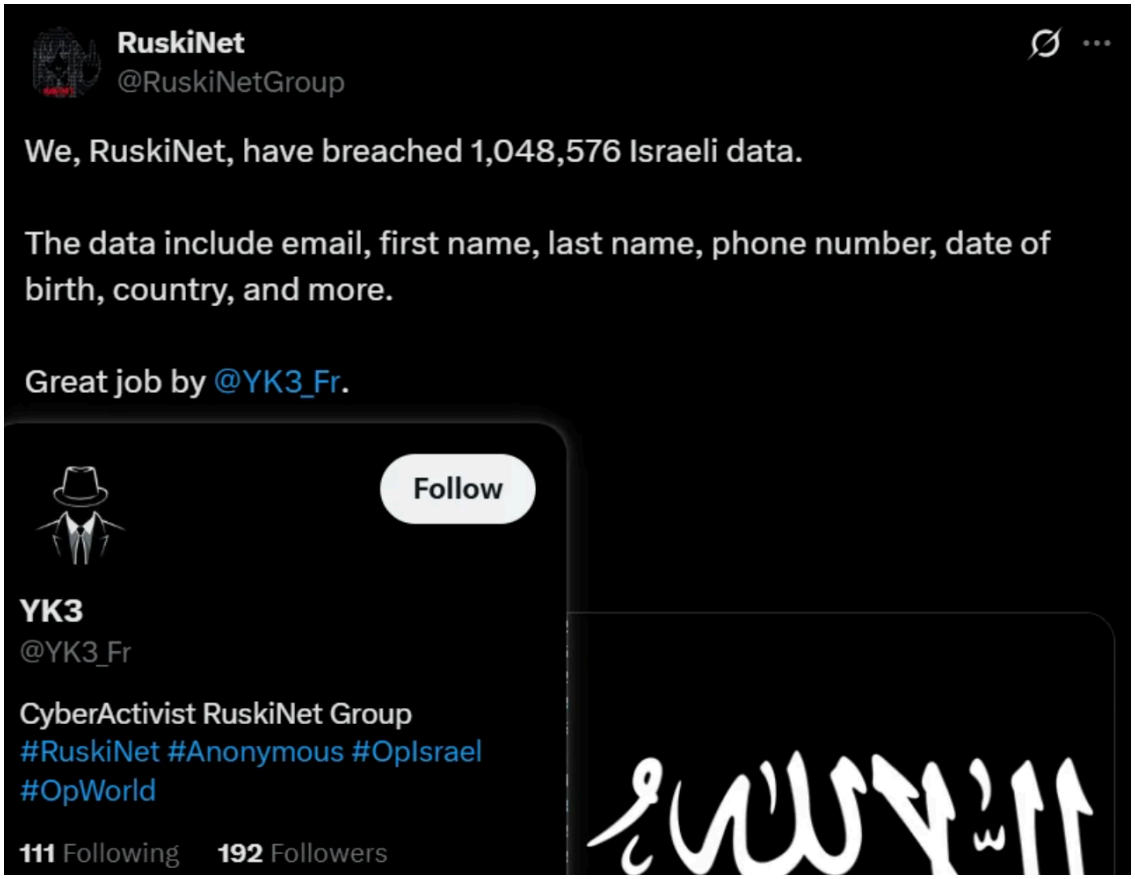
Figure 3. A diagram showing how MikroTik routers were used for DDoS attacks. Source: Cybernews

It‘s believed that the RuskiNet botnets have been used to send tens of thousands of spoofed emails containing trojans or ransomware payloads. Botnets also make DDoS attacks faster and more effective to coordinate.

An indictment by the US Attorney‘s Office in May 2025 charged 16 defendants in connection with a DanaBot malware network, infecting more than 300,000 victim computers globally.

4. Recycled data attacks

In June 2025, a threat actor under the alias “YK3” claimed to have leaked data belonging to 38,000 employees of SAP Israel. The threat actor‘s claim was reposted by RuskiNet on X, linking the hacker group to the breach.



An X post by RuskiNet claiming the DDoS attack on SAP Israel, performed by hacker YK3.

After further investigation, it was revealed that the alleged data breach was actually recycled information from a previously known data leak from October 2023, originally associated with an Israeli digital payments platform.

Alliances

Although unconfirmed publicly, many analysts have speculated that RuskiNet is working in tandem with other cybercriminal gangs to perpetrate attacks.

MoroccanCyberForces

In the wake of the African Cybersecurity Forum 2025 in Rabat, Morocco, the government made strides towards a pan-African cooperation in digital infrastructure for defense, with Russian delegates present to discuss initiatives for joint Russian-African energy infrastructure protection.

After the summit held in February, Morocco experienced a surge in cyberattacks, reportedly over 75,000 Distributed Denial-of-Service (DDoS) attacks, ranking second in Africa. Around the time of RuskiNet‘s most prolific attacks in June 2025, Morocco had reported a further 20.7 million attempted cyberattacks.

Russia has demonstrated its interest in participating in Morocco‘s rapidly expanding cyber defense strategy, offering cybersecurity tools and cooperation. From there, Morocco acts as a foothold into a broader global energy supply chain. Morocco, if it rejects Russia‘s support, could threaten Russian interests in the region.

MoroccanCyberForces emerged following the leak of sensitive data from Morocco's National Social Security Fund (CNSS) in early 2025 by Algerian hackers as tensions between the two countries rose. In retaliation, MoroccanCyberForces leaked data from Algeria's Ministry of Posts and Telecommunications (MGPTT).

The hacktivist's main goal is to protect Moroccan digital sovereignty, focusing on government agencies, infrastructure systems, and diplomatic entities.

Both RuskiNet and MoroccanCyberForces have a shared interest in both Russia's influence in Africa and Moroccan digital independence from larger global powers like the US.

RuskiNet is known for DDoS attacks, suggesting cooperation due to the large volume of DDoS attacks during 2025. MoroccanCyberForces similarly works to spread disinformation, defaces government websites, and focuses on operational disruption.

No official links have been made between the two hacktivist groups publicly, and information about the involvement between the two continues to evolve.

LockBit

LockBit, a cybercriminal group specializing in Ransomware-as-a-Service (RaaS), used double extortion tactics and social engineering in their cyberattacks. In May 2025, the group was breached and taken down by law enforcement.

While there's no confirmed link between RuskiNet and LockBit, overlapping infrastructure and shared tactics show a different story.

Threat intelligence has revealed that both groups:

- Have a pro-Russian affiliation and aim to further Russian agendas.
- Use DDoS attacks, website defacement, and data leaks to intimidate victims.
- Launch attacks on critical infrastructure for geopolitical goals.
- Use similar tools and tactics, like botnets and encrypted C2 infrastructure.

Mapping RuskiNet onto the MITRE ATT&CK framework

MITRE ATT&CK's framework helps better understand RuskiNet's TTPs and supports threat hunting efforts.

RuskiNet threat actors use a variety of sophisticated techniques, tactics, and procedures (TTPs) that rely on social engineering and phishing to gain access.

Tactic	Technique	Explainer
Reconaissance	T1595 Active Scanning	Scans for vulnerable public-facing infrastructure, especially energy and government systems.

Tactic	Technique	Explainer
	T1589 Gather Victim Identity Information	Targets social media and public records to identify key personnel.
Resource Development	T1583.001 Acquire Infrastructure: Domains	Uses spoofed domains for phishing and malware delivery.
	T1583.006 Acquire Infrastructure: Web Services	Leverages dark web forums and Telegram for coordination.
Initial Access	T1566.001 Phishing: Spearphishing Attachment	Sends malware-laced documents via spoofed emails.
	T1190 Exploit Public-Facing Application	Targets misconfigured DNS and vulnerable routers.
Execution	T1059 Command and Scripting Interpreter	Uses PowerShell and Bash scripts for payload execution.
	T1203 Exploitation for Client Execution	Exploits browser and document reader vulnerabilities.
Persistence	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys	Ensures malware persistence on compromised systems.
	T1136 Create Account	Creates rogue accounts on compromised systems.
Privilege Escalation	T1068 Exploitation for Privilege Escalation	Uses known exploits to gain admin access.
Defense Evasion	T1070.004 Indicator Removal on Host: File Deletion	Deletes logs and artefacts post-attack.

Tactic	Technique	Explainer
	T1562.001 Impair Defenses: Disable or Modify Tools	Disables antivirus and monitoring tools.
Exfiltration	T1041 Exfiltration Over C2 Channel	Sends stolen data through encrypted C2 channels.
	T1048.003 Exfiltration Over Alternative Protocol: Custom Protocol	Uses custom DNS tunnelling for stealth.
Impact	T1499 Endpoint Denial of Service	Launches DDoS attacks on government and energy sites.
	T1491.001 Defacement: Internal Website Defacement	Defaces websites to intimidate victims.

Mitigation tips

Thwarting a potential RuskiNet breach relies on good cybersecurity hygiene, including zero-trust architecture.

According to the CISA, here is how you should react when facing cyber incidents from a Russian-allied adversary:

- To stop a DDoS attack, identify the source address via SIEM or another logging service. If the attack is launched from a single pool of IP addresses, these can be blocked manually. Enabling firewalls, restricting the amount of IP traffic, and notifying your internet service provider can prevent DDoS interference.
- Secure your backups offline to restore after website defacements. Scanning all backup data with an antivirus program can be useful to ensure backups are free of malware.
- Regularly update the web-server backend software to prevent exploitation with common CVEs.
- Ensure that your website Content Management System (CMS) is not accessible from the internet and is regularly updated. Attackers often use vulnerabilities in plugins and extensions to gain a foothold.

Stop advanced persistent threats with CybelAngel

Cyber espionage groups continue to grow and persist. RuskiNet, while elusive, has proven its effectiveness in disrupting daily business and harming countries across the globe.

Thwart hacktivist groups before they cause disruption and damage with our Cyber Threat Intelligence platform. CybelAngel can detect potential breaches within your ecosystem early, preventing exploitation, reputational damage, and regulatory penalties.

Source: https://cybelangel.com/blog/ruskinet-hacktivism-apt-threats/