Cyber Insight

PMHC KillNet and Black Skills entities

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Cyberdefense

Credits Orange Cyberdefense

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources. This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

Credits Orange Cyberdefense

Contextualization

KillNet, a pro-Russian hacktivist group that emerged in March 2022, has quickly established itself as a significant player in the geopolitical cyberspace. Primarily known for its distributed denial-of-service (DDoS) attacks, the group targets government institutions, critical infrastructure, and companies in Western countries that support Ukraine.

Its strategic transformation has been marked by the creation of two distinct entities, PMHC KillNet and Black Skills, reflecting a clear intent to professionalize and diversify its operational capabilities.

This evolution reflects KillNet's attempt to establish a more formal and professional structure, mirroring the concept of private military companies like the Wagner Group.

By creating PMHC KillNet and Black Skills, the group aims to diversify its capabilities beyond DDoS attacks, potentially offering cyber mercenary services and attracting more skilled hackers.

Credits Orange Cyberdefense

KillNet group

- Creation date: KillNet was reportedly created in 2022, emerging as a pro-Russian hacktivist group during the war in Ukraine
- Probable Origin: The group is likely originating from Russia or allied countries, operating with implicit or explicit support from pro-Kremlin entities.
- Main strategies:
  KillNet primarily uses DDoS (Distributed Denial of Service) attacks to disrupt online services of its targets.
- Geopolitical Motivation:
  The group defends Russian interests, targeting countries and organizations supporting Ukraine or opposing Kremlin policies.
- Characteristic:
  Originally, KillNet distinguished itself through its decentralized network organization and its use of volunteer hacktivists to amplify its attacks, but it later became more structured.
- Targeted business sectors:
  The group mainly targets government, financial, health, and media sectors in Western countries and NATO allies.

Identification

Credits Orange Cyberdefense

Black Skills entity

- Creation date: Announced on March 13, 2023, by its leader, KillMilk

- Probable Origin: Its probable origin is as an attempt to rebrand Killnet and attract Russian government support as a cyber mercenary group.

- Main strategies:
  The main strategies of BlackSkills include organizing into structured subgroups for payroll, public relations, technical support, pen testing, data collection, analysis, information operations, and targeting priority targets

- Geopolitical Motivation:
  BlackSkills' geopolitical motivations likely align with Russia's broader strategic objectives, focusing on targets in Ukraine and organizations in countries supporting Ukraine in the ongoing war.

- Characteristic:
  A key characteristic of BlackSkills is its aim to be the cyber equivalent of the Wagner Private Military Company, with its own unique laws, objectives, and emphasis on discipline and order within the Russian hacking community

- Targeted business sectors:
  to conduct operations against a wide range of targets, potentially with more sophisticated and destructive attacks compared to Killnet's previous focus on DDoS attacks.

Identification

Credits Orange Cyberdefense

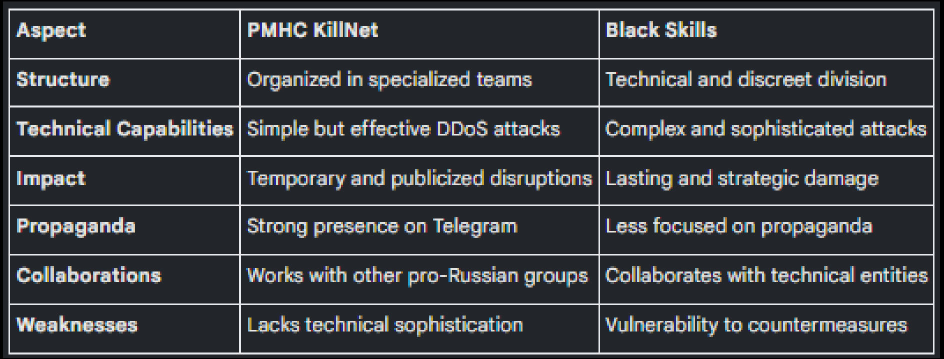
PMHC KillNet entity

- Creation date: PMHC KillNet (Private Military Hacker Company KillNet) was announced in April 2023 by Killmilk as a restructuring of the Killnet group
- Probable Origin: It's a hacktivist collective with unclear exact geographical origins, but it's strongly associated with international pro-Palestinian hacker networks.
- Main strategies:
  The main strategies of PMHC KillNet include offering "destructive" attacks against European and US targets, such as disinformation campaigns, attacks on network infrastructure, industrial sabotage, and reputational damage, as well as providing software development and non-cyber services like UAV (Unmanned Aerial Vehicles) production.
- Geopolitical Motivation:
  Likely align with Russian interests, as their targeting has consistently mirrored Russian strategic objectives and government rhetoric, supporting both external operations against perceived adversaries and internal promotion of support for Russia's actions in Ukraine
- Characteristic:
  Its shift from "altruism and hacktivism" to a profit-driven model, openly stating that they now take orders from private and government individuals while still claiming to defend Russian interests
- Targeted business sectors:
  Transportation, defense, government and military, financial services, global institutions, and telecommunications, with a particular focus on the U.S., Europe

Identification

Credits Orange Cyberdefense

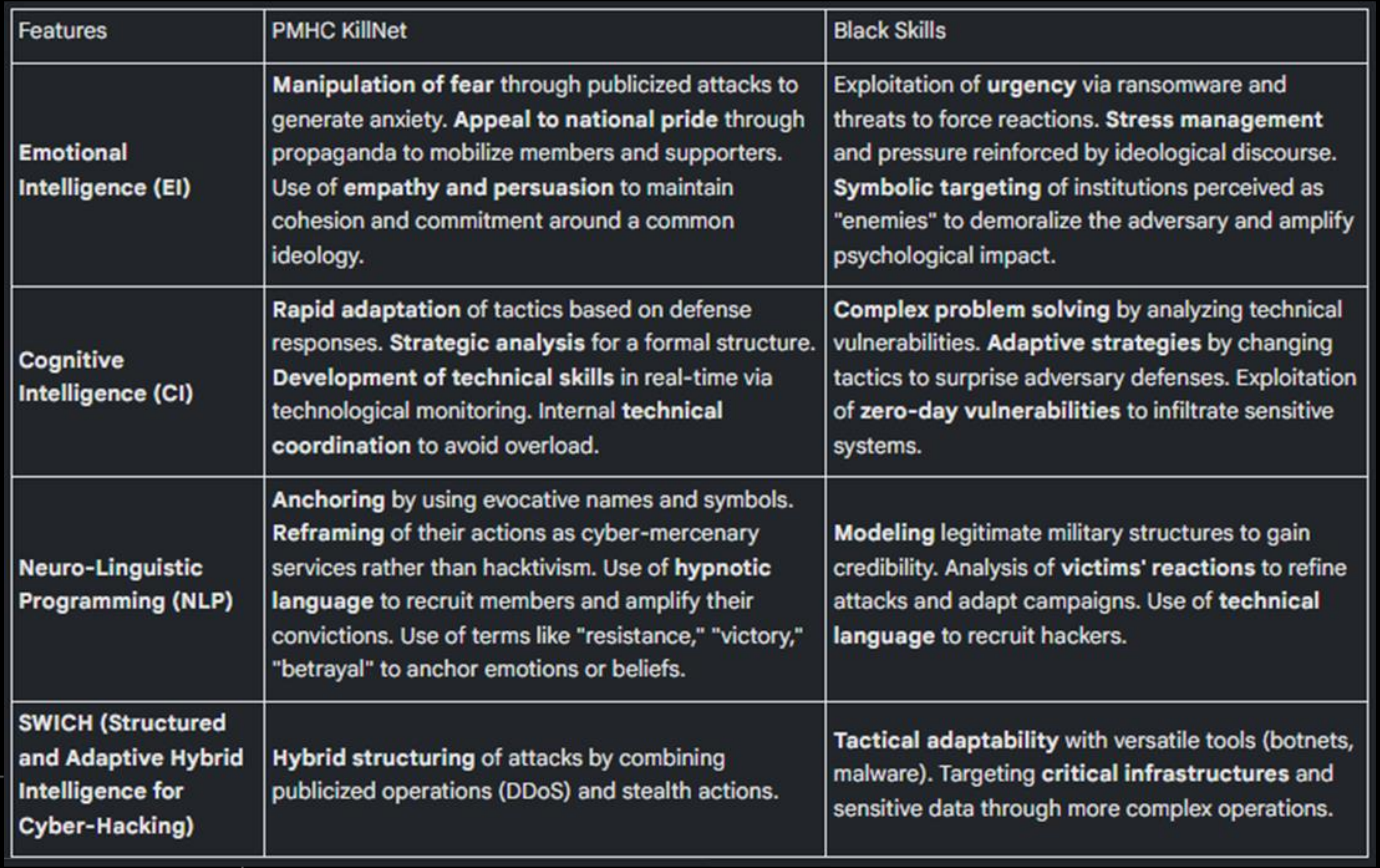
Growth Objectives for Both Entities



Aspect	PMHC KillNet	Black Skills
Structure	Organized in specialized teams	Technical and discreet division
Technical Capabilities	Simple but effective DDoS attacks	Complex and sophisticated attacks
Impact	Temporary and publicized disruptions	Lasting and strategic damage
Propaganda	Strong presence on Telegram	Less focused on propaganda
Collaborations	Works with other pro-Russian groups	Collaborates with technical entities
Weaknesses	Lacks technical sophistication	Vulnerability to countermeasures

Credits Orange Cyberdefense

Emotional, Cognitive Intelligence, NLP and SWICH



Features	PMHC KillNet	Black Skills
Emotional Intelligence (EI)	**Manipulation of fear** through publicized attacks to generate anxiety. **Appeal to national pride** through propaganda to mobilize members and supporters. Use of **empathy and persuasion** to maintain cohesion and commitment around a common ideology.	Exploitation of **urgency** via ransomware and threats to force reactions. **Stress management** and pressure reinforced by ideological discourse. **Symbolic targeting** of institutions perceived as "enemies" to demoralize the adversary and amplify psychological impact.
Cognitive Intelligence (CI)	**Rapid adaptation** of tactics based on defense responses. **Strategic analysis** for a formal structure. **Development of technical skills** in real-time via technological monitoring. Internal **technical coordination** to avoid overload.	**Complex problem solving** by analyzing technical vulnerabilities. **Adaptive strategies** by changing tactics to surprise adversary defenses. Exploitation of **zero-day vulnerabilities** to infiltrate sensitive systems.
Neuro-Linguistic Programming (NLP)	**Anchoring** by using evocative names and symbols. **Reframing** of their actions as cyber-mercenary services rather than hacktivism. Use of **hypnotic language** to recruit members and amplify their convictions. Use of terms like "resistance," "victory," "betrayal" to anchor emotions or beliefs.	**Modeling** legitimate military structures to gain credibility. Analysis of **victims' reactions** to refine attacks and adapt campaigns. Use of **technical language** to recruit hackers.
SWICH (Structured and Adaptive Hybrid Intelligence for Cyber-Hacking)	**Hybrid structuring** of attacks by combining publicized operations (DDoS) and stealth actions.	**Tactical adaptability** with versatile tools (botnets, malware). Targeting **critical infrastructures** and sensitive data through more complex operations.

Credits Orange Cyberdefense

Tools used by PMHC KillNet and Black Skills

- Aura-DDoS
- Blood
- DDoS Ripper
- Golden Eye
- Hasoki
- MHDDoS
- CC-Attack
- Killnet 2.0
- Passion Botnet
- Industroyer
- Triton
- Metasploit
- Cobalt Strike
- Tesla-Botnet
- Scripts DDoS
- Ransomware

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Governments and public institutions
- Critical infrastructures
- Healthcare and hospitals
- Financial services and banks
- Media and communication
- Education and research
- Technology and telecommunications
- Defense and military
- Transportation and logistics
- Energy and utilities
- International organizations
- Private sector and corporations

Note

Highly probable hybrid attacks through a combination of DDoS attacks by KillNet PMHC and sophisticated attacks by Black Skills, targeting critical infrastructure.

- Immediate threat: DDoS attacks against governments and media.
- Critical threat: Infiltration of energy infrastructures via malware.
- Strategic threat: Collaboration with state-sponsored groups for coordinated cyberattacks.

Credits Orange Cyberdefense

Targeted Countries

Romania

Ukraine

Czech Republic

Lithuania

Poland

United States

France

United Kingdom

Germany

Italy

Latvia

Japan

Norway

Estonia

Canada

Credits Orange Cyberdefense

Most Likely Hypothesis: Geopolitical Retaliation and Destabilization of Critical Infrastructure

The attacks are mainly motivated by retaliation against European countries supporting Ukraine and imposing sanctions on Russia. There is also a desire to destabilize these countries by targeting critical infrastructure.

Targets:

- Governments and public institutions: Websites, computer systems.
- Critical infrastructure: Energy networks, transportation systems, health services.
- Media: News agencies, communication platforms.
- Financial services: Banks and financial institutions.

Methods:

- DDoS attacks: Disruption of online services.
- Data exfiltration: Theft of sensitive data via ransomware or spyware.
- Phishing: Targeted phishing to steal login credentials.
- Exploitation of known vulnerabilities: Use of known security flaws.

Impacts:

- Disruption of public services: Limited access to government services.
- Destabilization of critical infrastructure: Potential for power outages, transportation disruptions, and disruptions to the healthcare system.
- Influence of public opinion: Attempts to manipulate information through disinformation.
- Economic weakening: Disruption of the financial sector and economic activity.

Credits Orange Cyberdefense

The most Dangerous Hypotheses

KillNet and its entities are potentially acting as proxies for the Russian government, with capabilities enhanced by the exploitation of unknown flaws and state collaborations.

Targets:

Sensitive critical infrastructure: Nuclear power plants, electrical networks, military systems.

Supply chains: Ports, railway networks.

Key governmental institutions: Defense systems, intelligence agencies.

Methods:

Exploitation of zero-day vulnerabilities: Use of unknown flaws to infiltrate the most sensitive systems.

Advanced malware: Deployment of malicious software specifically designed for critical infrastructures (e.g., Industroyer, Triton).

Attacks coupled with disinformation: Cyberattacks combined with fake news campaigns to amplify panic.

Collaboration with state actors: Direct or indirect support from the Russian government.

Impacts:

Massive power outages: Prolonged disruption of electrical services.

Economic destabilization: Paralysis of transportation infrastructure and supply chains.

Crisis of confidence: Loss of trust in institutions and governments.

Escalation of conflict: Potential for a hybrid cyberwar with major geopolitical implications.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

orange™ Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense