Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

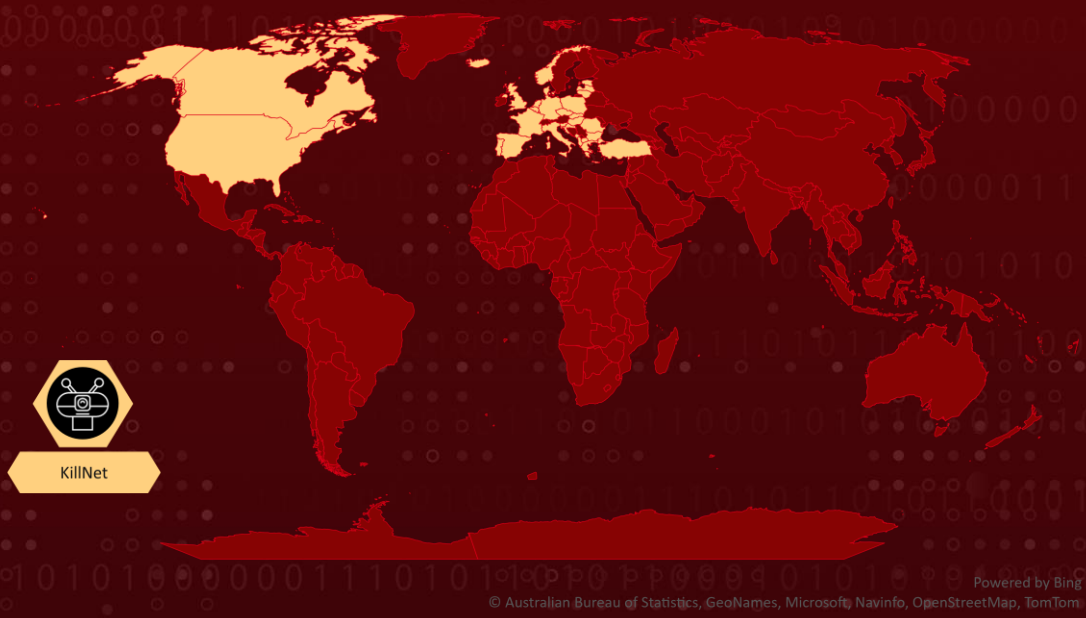
Russian Hacker Group Disrupts Relief Efforts for Turkey-Syria Earthquake with DDoS Attacks

Date of Publication	Admiralty Code	TA Number
February 14, 2023	A1	TA2023077

Summary

Attack Begin: February 2023
Threat Actor: KillNet
Attack Countries: NATO countries
Attack: Killnet, a Russian hacker group, disrupted relief efforts for the Turkey-Syria earthquake by carrying out DDoS attacks, taking down the websites of NATO Special Operations Headquarters and Strategic Airlift Capability.

Attack Regions



Attack Details

#1

Russian hacker group Killnet disrupted relief efforts for the Turkey-Syria earthquake by carrying out distributed denial of service (DDoS) attacks. They took down the website of NATO Special Operations Headquarters and Strategic Airlift Capability (SAC), among others, which impeded the efforts to provide aid. Killnet, a loosely organized group of pro-Kremlin activists, has been blamed for several cyberattacks, but they have not caused significant lasting damage.

#2

Although the attack only caused temporary outages, it warned SAC's C-17 aircraft of the disruption during a mission. NATO's cyber experts are actively addressing the issue and take cyber security very seriously. Killnet has clashed with pro-Western hacktivist collective Anonymous in the past and has been blamed for taking down several US hospitals' websites. They were responsible for a video released in March 2022, urging Russians to remain in the country and support the motherland during the Kremlin's invasion of Ukraine.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0006 Credential Access	TA0040 Impact
T1595 Active Scanning	T1589 Gather Victim Identity Information	T1583 Acquire Infrastructure	T1584 Compromise Infrastructure
T1110 Brute Force	T1498 Network Denial of Service	T1489 Service Stop	

References

https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

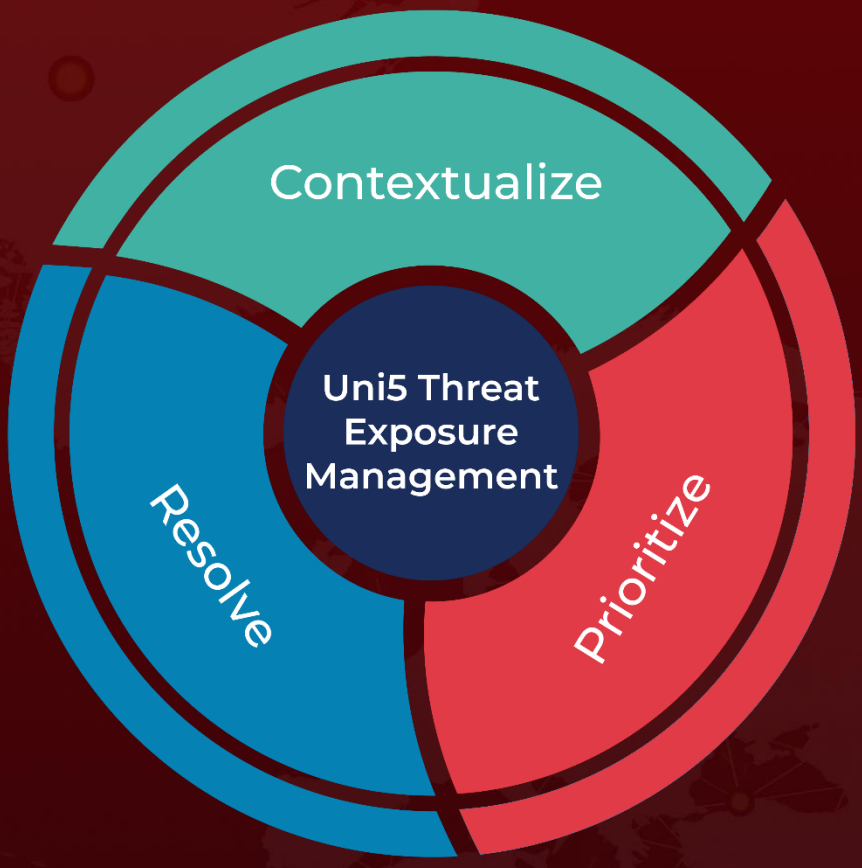
https://www.darkreading.com/attacks-breaches/russian-hackers-disrupt-nato-earthquake-relief-operations-

https://www.independent.co.uk/news/world/europe/turkey-syria-earthquake-russian-hackers-b2281278.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 14, 2023 • 12:45 AM

More at www.hivepro.com