Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Pro-Russian Hacktivist Group NoName057(16) Launches Cyber Attacks on Ukraine and NATO Organizations

Date of Publication	Admiralty code	TA Number
January 13, 2023	A1	TA2023023

Summary

First Appearance: March 2022
Actor Name: NoName057(16)
Target Regions: Ukraine and NATO
Target Sectors: Foreign Affairs, Shipping, Government, Critical Infrastructure, Financial

Actor Map

Actor Details

#1

NoName057(16) is a pro-Russian hacktivist group that has been conducting a campaign of DDoS attacks on Ukraine and NATO organizations since the early days of the war in Ukraine. The group has targeted government organizations and critical infrastructure and has been responsible for disrupting services across the financial sector of Denmark. It was also reported that on January 11th, NoName057(16) targeted 2023 Czech presidential election candidates' websites. The group operates through Telegram channels, a volunteer-fueled DDoS payment program, a multi-OS supported toolkit, and GitHub.

#2

The group's motivations are primarily focused on disrupting websites that are important to nations critical of Russia's invasion of Ukraine. The group's initial attacks were focused on Ukrainian news websites but later shifted to NATO-associated targets. However, their Telegram engagement has been in decline, suggesting that the group is becoming less relevant and impactful compared to other hacktivist groups.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
NoName057(16)[NoName05716, 05716nnm , Nnm05716]	Russia	Ukraine and NATO countries	Foreign Affairs, Shipping, Government, Critical Infrastructure, Financial
	MOTIVE		
	Hacktivist & Destruction		

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 actor 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

TA0011 Command and Control	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0007** Discovery
TA0040 Impact	**T1499** Endpoint Denial of Service	**T1498** Network Denial of Service	**T1049** System Network Connections Discovery
T1016 System Network Configuration Discovery	**T1547** Boot or Logon Autostart Execution	**T1071** Application Layer Protocol	

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	94d7653ff2f4348ff38ff80098682242ece6c407 e786c3a60e591dec8f4c15571dbb536a44f861c5 c86ae9efcd838d7e0e6d5845908f7d09aa2c09f5 e78ac830ddc7105290af4c1610482a41771d753f 09a3b689a5077bd89331acd157ebe621c8714a89 8f0b4a8c8829a9a944b8417e1609812b2a0ebbbd 717a034becc125e88dbc85de13e8d650bee907ea ef7b0c626f55e0b13fb1dcf8f6601068b75dc205 b63ce73842e7662f3d48c5b6f60a47e7e2437a11 5880d25a8fbe14fe7e20d2751c2b963c85c7d8aa 78248539792bfad732c57c4eec814531642e72a0 1dfc6f6c35e76239a35bfaf0b5a9ec65f8f50522
IPV4	2[.]57[.]122[.]82 2[.]57[.]122[.]243 109[.]107[.]181[.]130 77[.]91[.]122[.]69 31[.]13[.]195[.]87
Domain	tom56gaz6poh13f28[.]myftp.org zig35m48zur14nel40[.]myftp.org 05716nnm@proton[.]me dddosia[.]github.io

TYPE	VALUE
URLs	hxxps://t[.]me/noname05716 hxxps://t[.]me/nn05716chat hxxps://github[.]com/dddosia hxxps://github[.]com/kintechi341

Recent Breaches

https://www.jyskebank.dk/

https://www.sydbank.com/

References

https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/

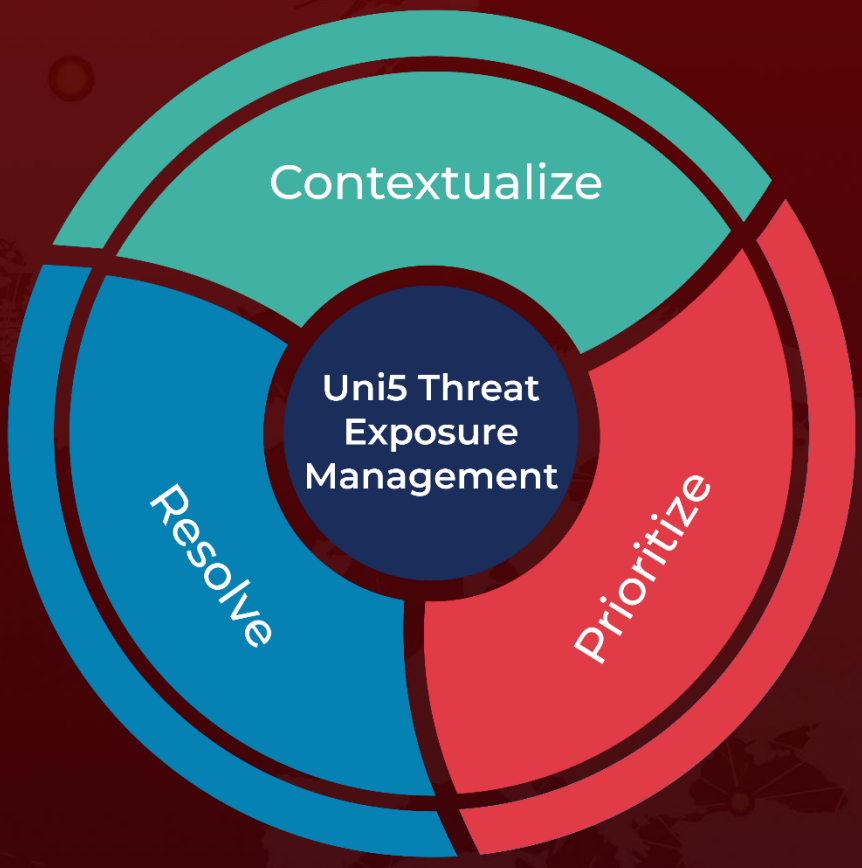
https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/

https://www.gov.pl/web/special-services/russian-cyberattacks

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

January 13, 2023 • 4:20 AM

More at www.hivepro.com