Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

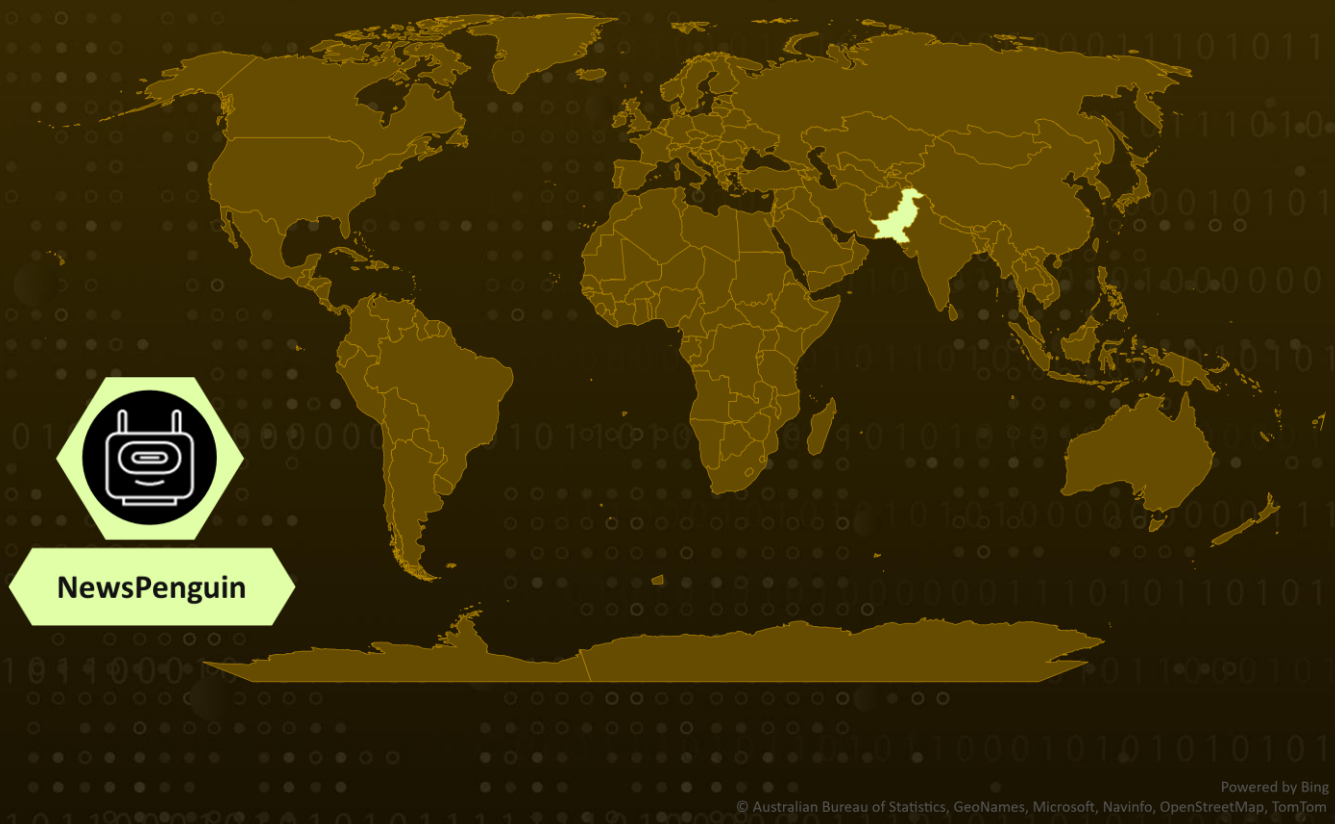
NewsPenguin Threat Actor Unleashes Malicious Attacks on Pakistani Firms

Date of Publication	Admiralty Code	TA Number
February 10, 2023	A1	TA2023074

Summary

First Appearance: February 2023
Actor Name: NewsPenguin
Target Region: Pakistan
Target Sectors: Defense, Government, Maritime, and Shipbuilding

Actor Map



Actor Details

#1

NewsPenguin is using a weaponized spear-phishing document as its attack vector, which is being distributed as an "exhibitor manual" aimed at visitors of the Pakistan International Maritime Expo & Conference (PIMEC)-23 event. The document, entitled "Important Document.doc," utilizes a remote template injection technique and contains malicious Visual Basic for Applications (VBA) macro code, enabling the delivery of the subsequent stage of the attack.

#2

When the victim activates "Enable Content," it triggers the execution of the malicious VBA macro code. This causes the macro to save a "test.dotx" file in rich text format (RTF). The payload is then downloaded and decoded from base64, and the final payload, an advanced espionage tool, is executed. This payload is XOR encrypted with a unique "penguin" encryption key.

#3

An innovative and previously undisclosed espionage tool has been discovered, equipped with a vast array of capabilities for bypassing security measures such as sandboxes and virtual machines. The attacker's methodology and preparation for this campaign indicate a continuous improvement of their tools and techniques to penetrate victim systems. Advanced planning, including the establishment of network infrastructure months before an event, is uncommon among criminal organizations.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
NewsPenguin	Unknown	Pakistan	Defense, Government, Maritime and Shipbuilding.
	MOTIVE		
	Information theft and espionage		

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

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0008 Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
T1137 Office Application Startup	**T1553** Subvert Trust Controls	**T1027** Obfuscated Files or Information	**T1029** Scheduled Transfer
T1036 Masquerading	**T1041** Exfiltration Over C2 Channel	**T1047** Windows Management Instrumentation	**T1055** Process Injection
T1055.002 Portable Executable Injection	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic	**T1059.003** Windows Command Shell
T1059.001 PowerShell	**T1083** File and Directory Discovery	**T1105** Ingress Tool Transfer	**T1112** Modify Registry

T1132 Data Encoding	**T1140** Deobfuscate/Decode Files or Information	**T1203** Exploitation for Client Execution	**T1204** User Execution
T1204.002 Malicious File	**T1480** Execution Guardrails	**T1497** Virtualization/Sandbox Evasion	**T1559** Inter-Process Communication
T1559.001 Component Object Model	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1221** Template Injection
T1573 Encrypted Channel	**T1491** Defacement	**T1070** Indicator Removal	**T1070.004** File Deletion
T1082 System Information Discovery	**T1564** Hide Artifacts	**T1057** Process Discovery	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	51.222.103[.]8 185.198.59[.]109
SHA256	80326b1e151e8348307114c8115e275c2fd63f0d2eb1dfacb6eca9840cf98525 26b113ba29b037034ee34a7f0fea81f6d5452950e0d26058d9b96946d78570c5 facb0bfb3123540415b28881bcf951b29ccdd3abace54747d76f19017e80e8d9 b4e22ffcaa349618342a933c2cc72896e8273c2095a1f232d7e34b119f485595 3F9FAC91288139F81D4949CD5DADDC131AA3443D2A8631093D971B2EBDE6AE77 55F43319B910037D5B2EB8A5E57A14FCA88E22BB0F40E453E510CC375A42BF43 EA732F213FCFC27E386471C290A342B7905FF8030888979D8220403A94D2CDCD 4C003C63F1A7C6D2EAEEB18D37B3EE824C82E1C0C44458A9510EF28C265962C6 538BB2540AAD0DCB512C6F0023607382456F9037D869B4BF00BCBDB18856B338

TYPE	VALUE
MD5	fcae6b88640b58d289df42ae2d15e3ca 28e5fceaa9878bfbe967639cf2a2fb9b 5abd9f1828e3c6d899b9c8ba79c16473 1cb100825912dd70c3a8f8e11fadc97f C219A8C50624F9DD9FC0F3C32510EA77 314328E63B2E55A9C20BBDA313AB4D04 8B0BF3F5F0AC4605C8C5EF73EB121757 861B80A75ECFB083C46F6E52277B69A9
SHA1	BFEC9148F90D1565AE334302D79B890964DD4C89
URLs	hxxp[:]//windowsupdates[.]shop/test[.]dotx hxxp[:]//updates.win32[.]live
Mutex	Windows.20H2.85685475

References

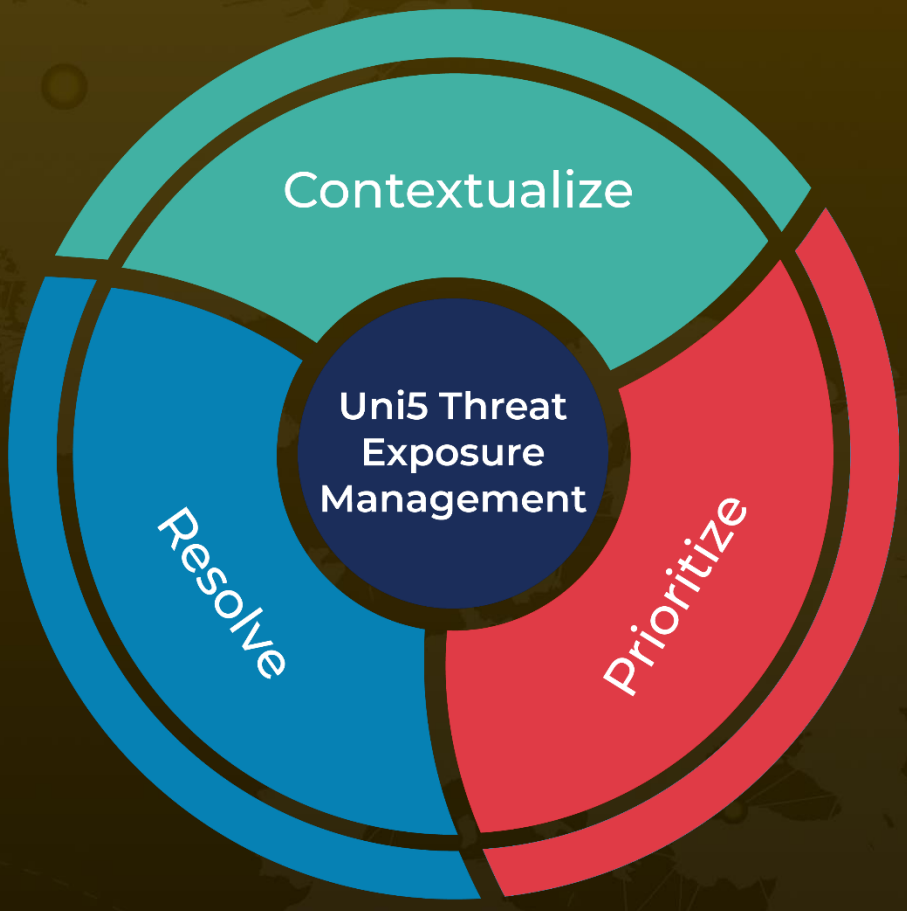
https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool

https://thehackernews.com/2023/02/newspenguin-threat-actor-emerges-with.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 10, 2023 • 2:39 AM

More at www.hivepro.com