Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

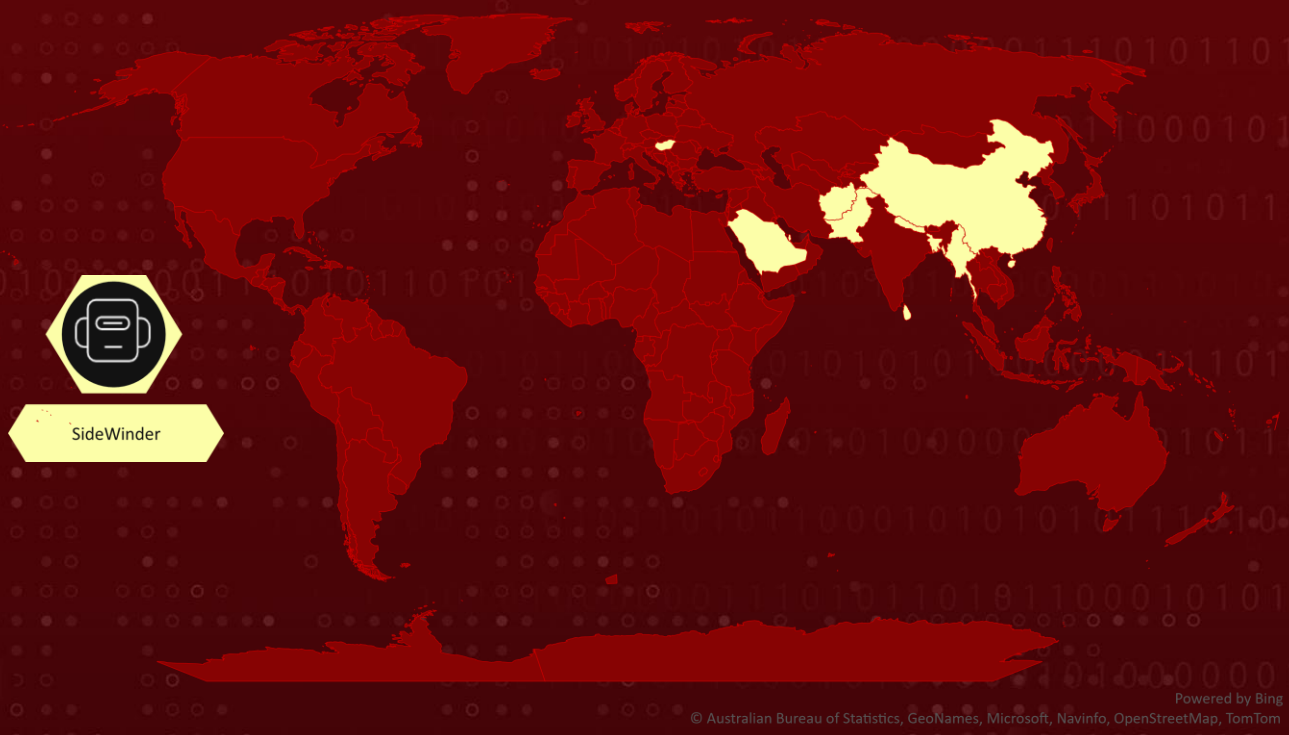
SideWinder APT group's new arsenal named WarHawk

Date of Publication	Admiralty code	TA Number
October 26, 2022	A1	TA2022232

Summary

The SideWinder APT gang operates espionage campaigns against government, military, and business sectors throughout Asia, primarily Pakistan, by employing the WarHawk backdoor to exfiltrate vulnerable system metadata to a remote server.

Actor Map



Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0011** Command and Control
TA0010 Exfiltration	**T1566** Phishing	**T1190** Exploit Public-Facing Application	**T1204** User Execution
T1059 Command and Scripting Interpreter	**T1140** Deobfuscate/Decode Files or Information	**T1564** Hide Artifacts	**T1055** Process Injection
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1041** Exfiltration Over C2 Channel	

Technical Details

#1

SideWinder APT exploited the official website of Pakistan's National Electric Power Regulatory Authority (NEPRA) to host an ISO file and transmit the new WarHawk backdoor, which contained several malicious modules that delivered Cobalt Strike Loader.

#2

The downloaded ISO file includes three malicious files: an LNK file, a decoy PDF, and a malicious binary. The WarHawk Backdoor masquerades as a legitimate app to trick unwary victims into execution. The malware consists of a command execution module capable of executing system commands from the infected computer's command-and-control server.

Actor Detail

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
SideWinder (Rattlesnake,T-APT-04,APT-C-17, Razor Tiger, Baby Elephant , Operation Origami)	India	Afghanistan, Bangladesh, China, Hungary, Myanmar, Nepal, Pakistan, Qatar, Saudi Arabia , Sri Lanka	Defense , Government, Hospitality , Legal , Transportation
	MOTIVE		
	Information theft and espionage		

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	d510808a743e6afc705fc648ca7f896a,63d6d8213d9cc070b2a3dfd3c5866564,8f9cf5c828cb02c83f8df52ccae03e2a,5cff6896e0505e8d6d98bff35d10c43a,ec33c5e1773b510e323bea8f70dcddb0, d0acccab52778b77c96346194e38b244,40f86b56ab79e94893e4c6f1a0a099a1

TYPE	VALUE
URLs	nepra[.]org[.]pk/css/32-Advisory-No-32[.]iso 146[.]190[.]235[.]137/Snitch[.]exe 146[.]190[.]235[.]137/OneDrive[.]exe 146[.]190[.]235[.]137/DDRA[.]exe

References

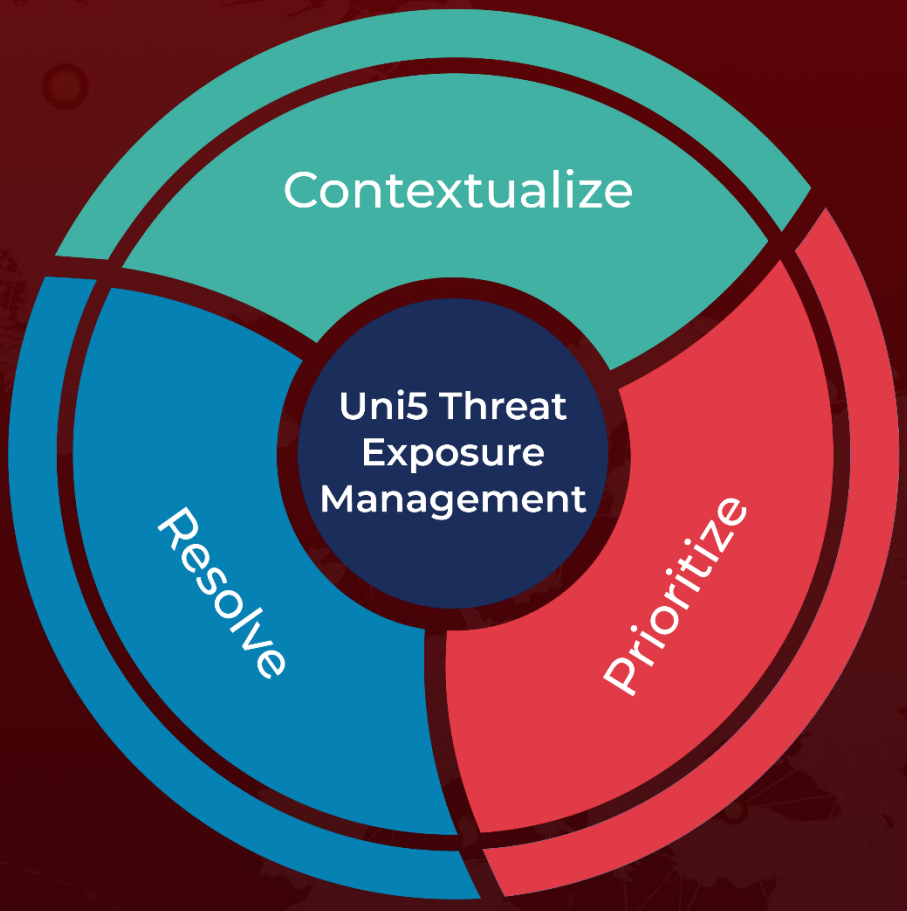
https://www.zscaler.com/blogs/security-research/warhawk-new-backdoor-arsenal-sidewinder-apt-group-0

https://thehackernews.com/2022/10/sidewinder-apt-using-new-warhawk.html

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

October 26, 2022 • 4:23 AM

More at www.hivepro.com