Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

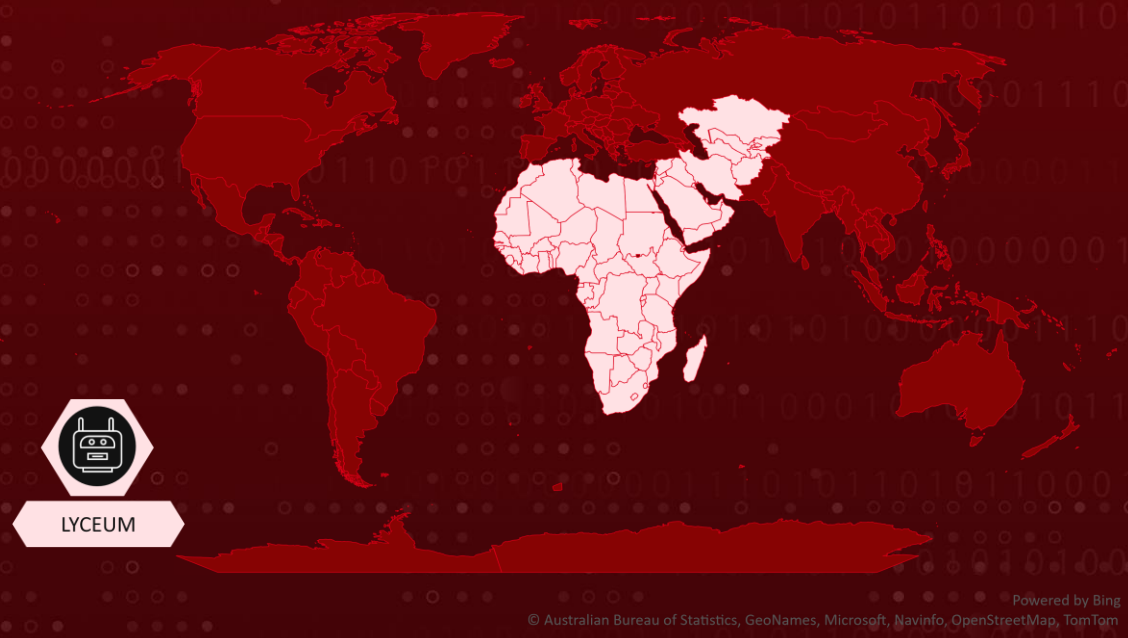
Iranian APT targets Middle East's Energy & Telecommunications industry

Date of Publication	Admiralty code	TA Number
June 20, 2022	A1	TA2022128

Summary

A new campaign has been launched by a state-sponsored Iranian APT group, Lyceum to target organizations from Middle East in the energy and telecommunication sectors. They have been observed deploying a new .NET based malware.

Actor Map



Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0007** Discovery	**TA0002** Execution	**TA0004** Privilege Escalation
TA0011 Command and Control	**T1055** Process Injection	**T1057** Process Discovery	**T1562** Disable or Modify Tools
T1059 Command and Scripting Interpreter	**T1018** Remote System Discovery	**T1518** Security Software Discovery	**T1010** Application Window Discovery
T1071 Application Layer Protocol			

Technical Details

#1 Lyceum, an APT group has developed a new .NET based DNS backdoor. This DNS backdoor is used to perform a DNS hijacking attack and has its code taken from an open-source tool DIG.net

#2 The attack chain begins by attacker sending spear-phishing attachment with a weaponized Word document. Once the user opens and enables macros in that document the DNS backdoor is dropped in the victim's system. This backdoor has the capabilities to upload/ download files and execute commands on the vulnerable system.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
LYCEUM (Hexane, Cobalt Lyceum, Siamesekitten, ATK 120)	Iran	Information theft and espionage	Israel, Kuwait, Morocco, Saudi Arabia, Tunisia, UAE and Middle East, Central Asia and Africa.	Energy, Oil and gas, Telecommunications

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	13814a190f61b36aff24d6aa1de56fe2 8199f14502e80581000bd5b3bda250ee
Domain	cyberclub[.]one hxxp://news-spot[.]live/Reports/1/?id=1111&pid=a52 hxxp://news-spot[.]live/Reports/1/?id=1111&pid=a28 hxxp://news-spot[.]live/Reports/1/?id=1111&pid=a40 hxxp://news-spot[.]live/Reports/1/45/DnsSystem[.]exe

References

https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 20, 2022. 5:00 AM

More at www.hivepro.com