Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

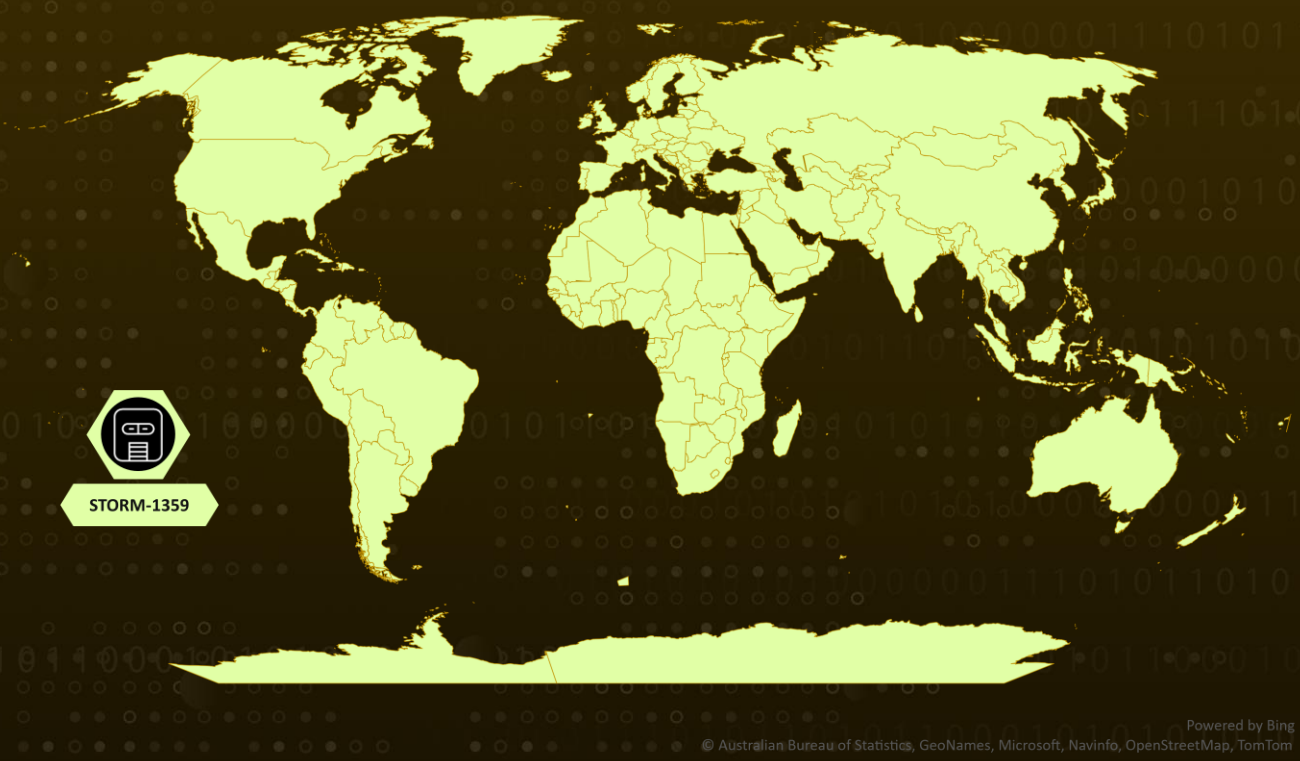
STORM-1359 DDoS triggered outage of Microsoft Services

Date of Publication	Admiralty Code	TA Number
June 20, 2023	A1	TA2023269

Summary

First appeared: January,2023
Attack Region: Worldwide
Targeted Industries: Technology Companies, Government Organisation, Aviation
Actor Name: STORM-1359 a.k.a. Anonymous Sudan
Attack: The STORM-1359 group recently targeted Microsoft services with a DDoS attack, resulting in the disruption of multiple services.

Attack Regions



Attack Details

#1 Microsoft services, including Azure, Outlook, OneDrive were inaccessible to number of users in early June. The service outage was due to traffic influx and Attacker Group a.k.a. Anonymous Sudan claimed the responsibility. The attack caused only Service unavailability and there is no evidence of any data breach.

#2 STORM-1359 established in January 2023 and since then have carried out multiple DDoS attacks on government agencies, Medical Facilities and number of other organizations. Recently, group has targeted UAE First Abu Dhabi Bank and caused service outage. They are associated with KillNet group.

#3 The attackers ran the DDoS attack through rented cloud infrastructure and virtual private and evaded CDN layer through cache bypass technique. Furthermore, the attackers executed Slowloris attacks, depleting the web server's resources and leading to a denial of service.

#4 Distributed Denial of Service attack involves engaging system with large number of request from multiple IP's, causing system to be busy for genuine request. Attackers were able to successfully utilize decade old L7 DDoS technique.

Recommendations

Enable Rate Limiting: Rate Limiting of user request helps in restricting no of request and thus prevents overwhelming network and resources.

Keep Watch on bots: Enable Anti-bot protection in perimeter security device to avoid bot consuming the network and resources

Review DDoS Protection: Review current security posture to eliminate DDoS attacks originating at various layers.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0040 Impact
T1491 Defacement	TA0007 Discovery	T1526 Cloud Service Discovery	T1590 Gather Victim Network Information
T1498 Network Denial of Service	T1583 Acquire Infrastructure	T1190 Exploit Public-Facing Application	

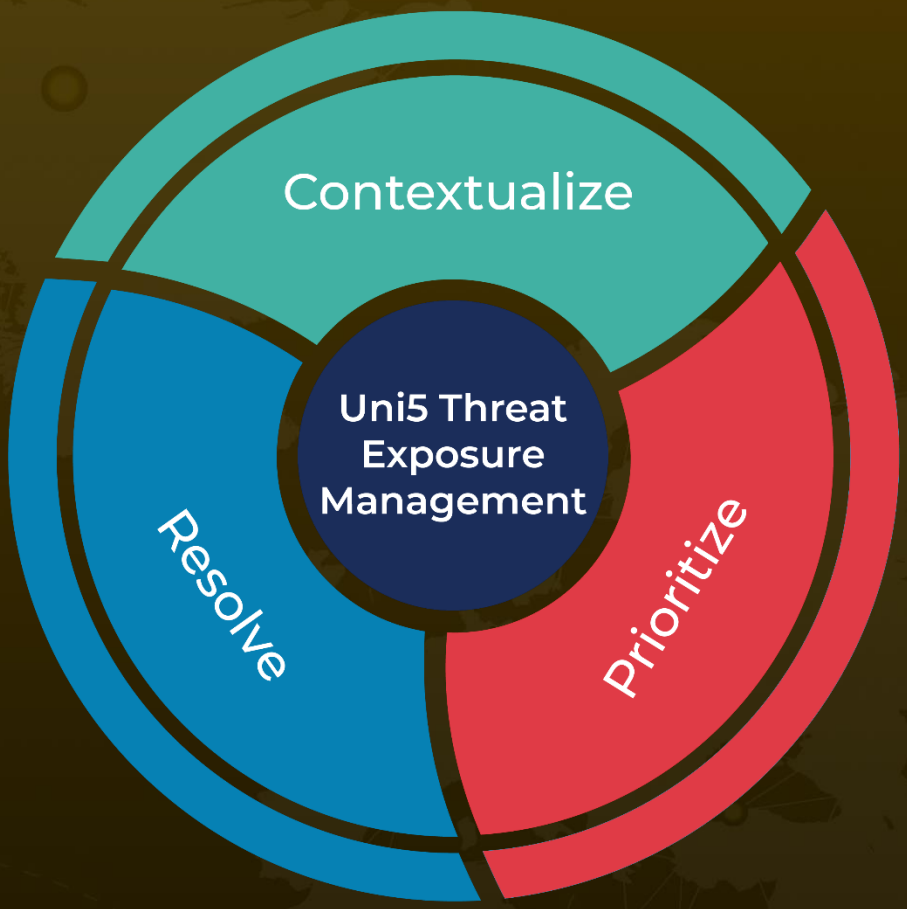
References

https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/

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

June 20, 2023 • 00:30 AM

More at www.hivepro.com