UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0329

MICROSOFT OUTAGES CAUSED BY DDOS ATTACKS

DATE ISSUED: 21st June 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Microsoft has confirmed that Layer 7 Distributed Denial-of-Service (DDoS) attacks indeed caused the recent outages affecting Azure, Outlook, and OneDrive web portals. A hacking group has claimed responsibility for flooding the sites with junk traffic in DDoS attacks.

BREAKDOWN

At the beginning of June, Microsoft's Office suite – including Outlook and OneDrive, became a target of a DDoS attack rendering the services unavailable to its users. According to a recent post from Microsoft Security Response Center, Microsoft has confirmed that the outages experienced were a direct result of a Layer 7 DDoS attack targeting their services. The attack was attributed to a threat actor identified by Microsoft as Storm-1359. No customer data is known to have been compromised. DDoS attacks pose significant threats to businesses as these attacks involve overwhelming a targeted network, server, or website with excessive traffic, rendering it inaccessible to legitimate users. Customer trust and confidence can be undermined when services are unavailable or unreliable, potentially resulting in customer's abandoning your services and reputational damage.

REMEDIATION STEPS

- Ensure that the mail filter provider has mail spooling capability to temporarily store incoming emails in a queue or buffer when the email server is unavailable or experiencing issues.
- Adequately backup the Office 365 environment by engaging with a reliable third-party provider for backup services.
- Regularly apply the latest updates provided by Microsoft to ensure that the Office 365 desktop apps are equipped with the most recent bug fixes and security enhancements.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-azure-outlook-outages-caused-by-ddos-attacks/

Security Week https://www.securityweek.com/microsoft-says-early-june-disruptions-to-outlook-cloud-platform-were-cyberattacks/amp/