U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00057

## MICROSOFT APT'S TARGET ENTERPRISE PLATFORMS

DATE ISSUED: 27th October 2020

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | [✓ HIGH] |
| EASE OF EXPLOIT | HARD | MEDIUM | [✓ EASY] |

## OVERVIEW

Targeting Microsoft services such as Exchange, Calendar and Outlook Web Access is the new tactic in avoiding detection for Advanced Persistent Threat attacks to steal sensitive business data and credentials.

## BREAKDOWN

Threat actors are evolving their tactics and leveraging web-facing, enterprise friendly Microsoft services in an effort to evade detection using new strains of malware. The Russian group known as Whitebear, Turla or Belugasturgeon has been known to target numerous government and public sector organizations using these particular services as a position from which to launch attacks, hide suspicious traffic, compromise emails and relay commands as well as harvest credentials and exfiltrate data. Another group dubbed "Sourface" have taken up similar tactics by manipulating local firewalls and using native commands and tools to proxy traffic across non-standard ports. IIS is also being observed to be an increasingly appealing target to deploy web shells to harvest credentials of those logging in to web-based services.

## REMEDIATION STEPS

- Isolate web-facing servers from the internal network using a DeMilitarised Zone or Zero-trust network architecture, separated by varied firewalls
- Always type the URL for Microsoft Online Services into the web browser address bar, rather than clicking links
- Use Web Application Firewall on any web-facing local servers
- Use role-based access controls and Privileged Identity Management as well as complex password policies
- Enable MFA on any accounts with administrative access to these services

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost | https://threatpost.com/microsoft-exchange-outlook-apts/160273/ |