FINISHED INTELLIGENCE REPORTS

HC3 Sector Alert: DHS Releases Cloud/Email Compromise Detection Tool Sparrow

TLP:WHITE

Dec 30, 2020

With recent reports indicating the compromise of Microsoft Azure/Office 365 services as an additional attack vector in the SolarWinds breach, the US Department of Homeland Security's

Cybersecurity & Infrastructure Security Agency (CISA) has created a free PowerShell-based tool used for the detection of potentially compromised applications and accounts in Azure/Microsoft 365 environments.

The tool, Sparrow, is intended for use by analysts, network defenders and incident responders. It is neither comprehensive nor exhaustive of available data, and is intended to narrow a larger set of available investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications. For more information, please reference the attached alert as well as Health-ISAC's briefing on the matter covered in the Daily Cyber Headlines available here.

Report Source(s)	HC3

Release Date
Dec 30, 2020

Alert ID 1e16e8ee

View Alert

Tags HC3

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the New Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, new notifications, and incident sharing in a trusted

environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.


For more update and alerts, visit: **https://health-isac.cyware.com**