Sector Alert
December 29, 2020

# Department of Homeland Security releases Cloud/Email compromise detection tool Sparrow

## Executive Summary

In mid-December 2020, it was widely reported that a highly sophisticated, large-scale, supply chain cyberattack was conducted against the SolarWinds Orion network management platform which likely impacted almost 18,000 customers. Victim organizations include both government and private sector, across many industry verticals including healthcare. The federal government continues to investigate the full scope of the campaign, as well as develop and highlight actions individual organizations can take to identify associated malicious activity and secure their infrastructure from future compromises. As part of this effort, the Department of Homeland Security (DHS) is releasing a free tool for detecting unusual and potentially malicious activity called Sparrow which can be found here.

## Analysis

The SolarWinds Orion attack has impacted both government and private sector targets and as such, DHS is maintaining a webpage with a summary of the ongoing events, a high-level overview titled, What Every Leader Needs to Know About the Ongoing APT Cyber Activity, as well as priority mitigation instructions included in Emergency Directive 21-01, which provides guidance in identifying threats, minimizing damage and protecting and organization's information infrastructure. During iterative releases of research and analysis of the cyberattack, Microsoft reported the targeting of identity management technologies, including stolen credentials and access tokens, and how they are being used to potentially compromise Microsoft's own cloud services customers, specifically accounts for Azure/Office365.

## Alert

With recent reports tying the SolarWind attack to compromise of Microsoft Azure/Office 365 services, the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has created a free PowerShell-based tool that helps detect potentially compromised applications and accounts in Azure/Microsoft 365 environments. The tool, Sparrow.ps1, is intended for use by analysts, network defenders and incident responders and 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", as described on the tool's public home page. The page also includes required permissions for Azure Active Directory and Microsoft Office365, installation and usage instructions as well as opportunities to contribute to the project. HHS recommends all healthcare organizations that believe they may be compromised by these attacks based on their infrastructure examine the Sparrow tool for use in assisting in these efforts.

## References

Microsoft: Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610

Microsoft: Important steps for customers to protect themselves from recent nation-state cyberattacks
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

CISA Releases Free Detection Tool for Azure/M365 Environment
https://us-cert.cisa.gov/ncas/current-activity/2020/12/24/cisa-releases-free-detection-tool-azurem365-environment

GitHub CISA: Sparrow.ps1
https://github.com/cisagov/Sparrow

What Every Leader Needs to Know About the Ongoing APT Cyber Activity
https://www.cisa.gov/insights

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | FireEye Inc