TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members and Intel Partners

DATE ISSUED: September 13, 2017

SUBJECT: DHS Issues Binding Operational Directive on Kaspersky Products

On September 13, 2017, the U.S. Department of Homeland Security (DHS) released Binding Operational Directive (BOD) 17-01 directing federal agencies to remove/discontinue use of products, solutions, and services provided by AO Kaspersky Lab or related entities. The BOD mandates that federal agencies identify Kaspersky Lab products on federal information systems within the next 30 days, develop detailed plans to remove and discontinue use of the products within 60 days, and implement those removal/discontinuation plans within 90 days. This follows the July 11, 2017, General Services Administration (GSA) decision to remove Kaspersky Lab from its list of approved vendors due to alleged ties between the company and Russian intelligence services.

DHS assesses that Kaspersky products, solutions, and services, supplied directly or indirectly by Kaspersky Lab or related entities, provide broad access to files and elevated privileges. The risks cited by DHS is twofold: that DHS is concerned with ties between Kaspersky Lab officials and that the Russian government and that Russian law could allow Russian intelligence or government agencies to request or compel assistance from Kaspersky Lab. These actions could result in the interception of U.S. communications transiting Russian networks and/or capitalize on the access provided to U.S. federal government networks through Kaspersky products.

RECOMMENDATIONS:
The MS-ISAC recommends members follow the guidance in the federal directive.

REFERENCES:
DHS Statement on BOD 17-01:
https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01