Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

December 29, 2016

Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity
On October 7, 2016, Secretary Johnson and Director Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts. The statement also noted that the Russians have used similar tactics and techniques across Europe and Eurasia to influence public opinion there.

Today, DHS and FBI released a Joint Analysis Report (JAR) which further expands on that statement by providing details of the tools and infrastructure used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political and private sector entities.

This activity by Russian intelligence services is part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. These cyber operations have included spearphishing, campaigns targeting government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the recent public release of some of this stolen information. In other countries, Russian intelligence services have also undertaken damaging and disruptive cyber-attacks, including on critical infrastructure, in some cases masquerading as third parties or hiding behind false online personas designed to cause victim to misattribute the source of the attack. The Joint Analysis Report provides technical indicators related to many of these operations, recommended mitigations and information on how to report such incidents to the U.S. Government.

A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies. The U.S. Government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies. The Joint Analysis Report recognizes the excellent work undertaken by security companies and private sector network owners and operators, and provides new indicators of compromise and malicious infrastructure identified during the course of investigations and incident response. The U.S. Government seeks to arm network defenders with the tools they need to identify,, detect and disrupt Russian malicious cyber activity that is targeting our country's and our

Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity

allies' networks.

We encourage security companies and private sector owners and operators to look back within their network traffic for signs of the malicious activity described in the Joint Analysis Report. We also encourage such entities to utilize these indicators in their proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to its Automated Indicator Sharing service, which provides indicators of malicious cyber activity at machine speed. Entities that are participating in this service have already implemented these indicators for the network protection activities.