TLP:WHITE

Russia Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a complete list of related CISA publications, many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Russian government actors). Additionally, this page provides instructions on how to report related threat activity.

The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.[1] Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing. The same reporting associated Russian actors with a range of high-profile malicious cyber activity, including the 2020 compromise of the SolarWinds software supply chain, the 2020 targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of U.S industrial control system infrastructure, the 2017 NotPetya ransomware attack on organizations worldwide, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee.

According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis." The Assessment states that "Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[2]

Latest U.S. Government Report on Russian Malicious Cyber Activity

On April 20, 2022, the cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom released a joint Cybersecurity Advisory to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners. The advisory provides an overview of Russian state-sponsored advanced persistent threat groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

The Russian Malicious Cyber Activity section below lists all CISA Advisories, Alerts, and Malware Analysis Reports (MARs) on Russian malicious cyber activities. See CISA.gov/supply-chain-compromise for additional partner products.

Expand All Sections

TLP:WHITE

Russian Malicious Cyber Activity

TLP:WHITE

Much of the information contained in the Advisories, Alerts, and MARs listed below is the result of analytic efforts between CISA, the U.S. Department of Defense (DoD), and the Federal Bureau of Investigation (FBI) to provide technical details on the tools and infrastructure used by Russian state-sponsored cyber actors. The publications below include descriptions of Russian malicious cyber activity, technical details, and recommended mitigations. Users and administrators should flag activity associated with the information in the products listed in table 1 below, report the activity to CISA or FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
April 20, 2022	• Joint Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure	The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom have released a joint Cybersecurity Advisory to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners. This advisory provides an overview of Russian state-sponsored advanced persistent threat groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

March 24, 2022	• Joint Cybersecurity Advisory: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector	This joint Cybersecurity Advisory—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)—provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations. CISA, the FBI, and DOE responded to these campaigns with appropriate action in and around the time that they occurred. CISA, the FBI, and DOE are sharing this information in order to highlight historical tactics, techniques, and procedures (TTPs) used by adversaries to target U.S. and international Energy Sector organizations. On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies.
March 15, 2022	• Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability	This Advisory warns organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default MFA protocols and a known vulnerability. As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization (NGO), allowing them to enroll a new device for MFA and access the victim network. The actors then exploited a critical Windows Print Spooler vulnerability, “PrintNightmare” (CVE-2021-34527) to run arbitrary code with system privileges. Russian state-sponsored cyber actors successfully exploited the vulnerability while targeting an NGO using Cisco’s Duo MFA, enabling access to cloud and email accounts for document exfiltration.
February 23, 2022	• Joint Cybersecurity Advisory: New Sandworm Malware Cyclops Blink Replaces VPNFilter	In this Advisory, NCSC-UK, CISA, NSA and the FBI report that the malicious cyber actor known as Sandworm or Voodoo Bear is using new malware, referred to as Cyclops Blink. Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, which exploited network devices, primarily small office/home office routers and network-attached storage devices.

February 16, 2022	• Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology	From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. This Advisory provides detection and mitigation recommendations for CDCs to reduce the risk of data exfiltration by Russian state-sponsored actors.
January 11, 2022	• Joint Cybersecurity Advisory: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure	This Advisory provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. It is intended to help the cybersecurity community reduce the risk presented by these threats.
July 20, 2021	• ICS Advisory: ICSA-14-178-01: ICS Focused Malware – Havex • ICS Alert: ICS-ALERT-14-281-01E: Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) • ICS Alert: IR-ALERT-H-16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure • Technical Alert: TA17-163A: CrashOverride Malware	These previously published ICS advisories and alerts contain information on historical cyber-intrusion campaigns by Russian nation-state cyber actors.
July 16, 2021	• Joint Cybersecurity Advisory: APT29 targets COVID-19 vaccine development	This Advisory details recent Tactics, Techniques and Procedures (TTPs) of the group commonly known as ‘APT29’, also known as ‘the Dukes’ or ‘Cozy Bear’. It also provides indicators of compromise as well as detection and mitigation advice.

July 1, 2021	• Joint Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments	This Advisory details how the Russian General Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) has targeted hundreds of U.S. and foreign organizations using brute force access to penetrate government and private sector victim networks. The advisory reveals the tactics, techniques, and procedures (TTPs) GTsSS actors used in their campaign to exploit targeted networks, access credentials, move laterally, and collect and exfiltrate data.
May 14, 2021	• CISA Analysis Report: Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise	This Analysis Report provides guidance to federal agencies in crafting eviction plans in response to the SolarWinds Orion supply chain compromise. The guidance is intended for federal agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity. Although this guidance is tailored to federal agencies, CISA encourages critical infrastructure entities; state, local, tribal, and territorial government organizations; and private sector organizations to review and apply it, as appropriate. **Note:** For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.
May 7, 2021	• Joint NCSC-CISA-FBI-NSA CSA: Further TTPs associated with SVR cyber actors	This Joint Cybersecurity Advisory (CSA) is on Russian SVR activities related to the SolarWinds Orion compromise. The CSA details SVR tactics, techniques, and procedures (TTPs) and on SVR-leveraged malware, including WELLMESS, WELLMAIL, GoldFinder, GoldMax, and possibly Sibot, as well as open-source Red Team command and control frameworks, Sliver and Cobalt Strike. **Note:** See FactSheet: Russian SVR Activities for summaries of three key Joint CSAs that detail Russian SVR activities related to the SolarWinds compromise. For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.
April 26, 2021	• Joint FBI-DHS-CISA CSA: SVR Cyber Operations: Trends and Best Practices for Network Defenders	This Joint CSA is on Russian SVR activities related to the SolarWinds Orion compromise. The CSA provides information on SVR TTPs. Specifically, this CSA points out the FBI's observation that, starting in 2018, the SVR shifted from "using malware on victim networks to targeting cloud resources, particularly e-mail, to obtain information." Significantly, SVR's compromise of Microsoft cloud environments following their SolarWinds Orion supply chain compromise is an example of this trend. **Note:** See FactSheet: Russian SVR Activities for summaries of three key Joint CSAs that detail Russian SVR activities related to the SolarWinds compromise. For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.

April 15, 2021	• Joint NSA-CISA-FBI CSA: Russian SVR Targets U.S. and Allied Networks	This Joint CSA is on Russian SVR activities related to the SolarWinds Orion compromise. The CSA details the vulnerabilities the SVR is leveraging—as well as the techniques it is using—in its attempts to compromise U.S. and Allied networks. **Note:** See FactSheet: Russian SVR Activities for summaries of three key Joint CSAs that detail Russian SVR activities related to the SolarWinds compromise. For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.
March 18, 2021	• CISA Alert: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool	This Alert announces the CISA Hunt and Incident Response Program (CHIRP) tool. CHIRP is a forensics collection tool that CISA developed to help network defenders find indicators of compromise (IOCs) associated with the SolarWinds Orion supply chain compromise. **Note:** For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.
January 8, 2021	• CISA Alert: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments	This Alert is a companion alert to CISA Alert: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. This Alert addresses the APT actor's tactics and techniques. **Note:** For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.
December 17, 2020	• CISA Alert: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations • MAR 10318845-1.v1 - SUNBURST • MAR 10320115-1.v1 - TEARDROP • MAR 10327841-1.v1 – SUNSHUTTLE	This Alert focuses on an APT actor’s compromise of SolarWinds Orion products affecting U.S. government agencies, critical infrastructure entities, and private network organizations. **Note:** For more information on the SolarWinds Orion supply chain compromise, refer to the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise webpage.

October 22, 2020	• Joint FBI-CISA CSA: Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets	This Joint CSA provides information on Russian state-sponsored APT actor activity targeting various U.S. state, local, tribal, and territorial government networks, as well as aviation networks. This Advisory updates Joint CISA-FBI CSA: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations.
October 9, 2020	• Joint CISA-FBI CSA: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations	This Joint CSA provides information on APT actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability. The commonly used tactic, known as vulnerability chaining, exploits multiple vulnerabilities in the course of a single intrusion to compromise a network or application.
April 16, 2018	• Joint DHS-FBI-NCSC Alert: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices	This Joint Technical Alert provides information on the worldwide cyber exploitation of network infrastructure devices by Russian state-sponsored cyber actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and the internet service providers supporting these sectors.
March 15, 2018	• Joint DHS-FBI Alert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors	This Joint Technical Alert provides information on Russian government actions targeting U.S. government entities as well as critical infrastructure organizations. It also contains IOCs and technical details on the TTPs used by Russian government cyber actors on compromised victim networks.

July 1, 2017	• CISA Alert: Petya Ransomware	This Technical Alert provides in-depth technical analysis of NotPetya malware, a Petya malware variant that surfaced on June 27, 2017. The U.S. Government has publicly attributed this NotPetya malware variant to the Russian military.
February 10, 2017	• CISA Analysis Report: Enhanced Analysis of GRIZZLY STEPPE Activity	This Analysis Report provides signatures and recommendations to detect and mitigate threats from GRIZZLY STEPPE actors.
December 29, 2016	• Joint DHS-FBI Analysis Report: GRIZZLY STEPPE - Russian Malicious Cyber Activity	This Joint Analysis Report provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Report Activity Related to This Threat

Mitigate and Detect This Threat

Respond to an Incident

References