Russian Threat Overview & Guidance on Adopting a Heighted Cyber Security Posture From Cybersecurity & Infrastructure Security Agency

CISA has webpages dedicated to the Russian threat overview and guidance on adopting a heighted cyber security posture.

Information Source: https://www.cisa.gov/uscert/russia & https://www.cisa.gov/shields-up

Provided below are a few key areas of the CISA website that may be of interest.

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 February 23, 2022, CISA, the United Kingdom's National Cyber Security Centre (NCSC-UK), National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory identifying that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to as Cyclops Blink. The NCSC, CISA, and FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST). See AA22-054A: New Sandworm Malware Cyclops Blink Replaces VPNFilter.

Russian Threat Overview & Guidance on Adopting a Heighted Cyber Security Posture From Cybersecurity & Infrastructure Security Agency

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.

Russia's unprovoked attack on Ukraine, which has been accompanied by cyber-attacks on Ukrainian government and critical infrastructure organizations, may have consequences for our own nation's critical infrastructure, a potential we've been warning about for months.

While there are no specific or credible cyber threats to the U.S. homeland at this time, we are mindful of the potential for Russia's destabilizing actions to impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity.

CISA, along with their partners in the U.S. Intelligence Community, law enforcement, the military, and sector risk management agencies, is monitoring the threat environment 24/7 to discern whether those threats manifest themselves in risks to the U.S. homeland.

In the wake of continued denial of service and destructive malware attacks affecting Ukraine and other countries in the region, we are working very closely with our Joint Cyber Defense Collaborative (JCDC) and international computer emergency readiness team (CERT) partners to understand and rapidly share information on these ongoing malicious cyber activities.

As the nation's cyber defense agency, CISA stands ready to help organizations respond to cyber-attacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

In today's highly connected and complex technology environment it has become increasingly challenging to completely prevent incidents that may disrupt business operations, especially given the dependencies on supply chains where there is inherently imperfect control.

This current environment requires us all to be laser-focused on resilience. This must include a focus on ensuring preparedness and a rapid, coordinated response to mitigate the impact of such disruptions on our national security, economic prosperity, or public health and safety.

Free cybersecurity services and toolsCISA has been working closely with our critical infrastructure partners over the past several months to ensure awareness of potential threats—part of a paradigm shift from being reactive to being proactive.

Russian Threat Overview & Guidance on Adopting a Heighted Cyber Security Posture From Cybersecurity & Infrastructure Security Agency

As part of this effort, CISA recognizes that many critical infrastructure or state, local, tribal, and territorial governments find it challenging to identify resources for urgent security improvements.

In response, CISA has established a catalog of free services from government partners, the open source community, and JCDC companies to assist with this critical need.

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Recommended actions include:

Reduce the likelihood of a damaging cyber intrusion

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. CISA also recommends organizations visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

Organization leaders have an important role to play in ensuring that their organization adopts a heightened security posture. CISA urges all senior leaders, including CEOs, to take the following steps:

- **Empower Chief Information Security Officers (CISO):** In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:** Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.
- **Participate in a Test of Response Plans:** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.
- **Focus on Continuity:** Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.
- **Plan for the Worst:** While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management

should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

As the nation's cyber defense agency, CISA is available to help organizations improve cybersecurity and resilience, including through cybersecurity experts assigned across the country. In the event of a cyber incident, CISA is able to offer assistance to victim organizations and use information from incident reports to protect other possible victims. All organizations should report incidents and anomalous activity to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.