# JOINT CYBERSECURITY ADVISORY

*Co-Authored by:*

TLP:WHITE

Product ID: AA22-110A

April 20, 2022

# Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

## SUMMARY

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is 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.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the

Actions critical infrastructure organizations should implement to immediately protect against Russian state-sponsored and criminal cyber threats:

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Enforce multifactor authentication.
- Secure and monitor remote desktop protocol and other risky services.
- Provide end-user awareness and training.

***U.S. organizations**: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov. **Australian organizations**: visit cyber.gov.au/acsc/report or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. **Canadian organizations**: report incidents by emailing CCCS at contact@cyber.gc.ca. **New Zealand organizations:** report cyber security incidents to ncscincidents@ncsc.govt.nz or call 04 498 7654. **United Kingdom organizations:** report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.*

March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing materiel support to Ukraine. Other cybercrime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive.

This advisory updates joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, which provides an overview of Russian state-sponsored cyber operations and commonly observed tactics, techniques, and procedures (TTPs). This CSA—coauthored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC)—provides an overview of Russian state-sponsored advanced persistent threat (APT) groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge critical infrastructure network defenders to prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity. Refer to the Mitigations section of this advisory for recommended hardening actions.

For more information on Russian state-sponsored cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage. For more information on the heightened cyber threat to critical infrastructure organizations, see the following resources:

- Cybersecurity and Infrastructure Security Agency (CISA) Shields Up and Shields Up Technical Guidance webpages
- Australian Cyber Security Centre's (ACSC) Advisory Australian Organisations Should Urgently Adopt an Enhanced Cyber Security Posture.
- Canadian Centre for Cyber Security (CCCS) Cyber Threat Bulletin Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity
- National Cyber Security Centre New Zealand (NZ NCSC) General Security Advisory Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine
- United Kingdom's National Cyber Security Centre (NCSC-UK) guidance on how to bolster cyber defences in light of the Russian cyber threat

# TECHNICAL DETAILS

## Russian State-Sponsored Cyber Operations

Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology (OT) networks; and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.

Historical operations have included deployment of destructive malware—including BlackEnergy and NotPetya—against Ukrainian government and critical infrastructure organizations. Recent Russian state-sponsored cyber operations have included DDoS attacks against Ukrainian organizations. **Note**: for more information on Russian state-sponsored cyber activity, including known TTPs, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.

Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- **The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18**
- **Russian Foreign Intelligence Service (SVR)**
- **Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)**
- **GRU's Main Center for Special Technologies (GTsST)**
- **Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)**

### *The Russian Federal Security Service*

**Overview:** FSB, the KGB's successor agency, has conducted malicious cyber operations targeting the Energy Sector, including UK and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. FSB has been known to task criminal hackers for espionage-focused cyber activity; these same hackers have separately been responsible for disruptive ransomware and phishing campaigns.

Industry reporting identifies three intrusion sets associated with the FSB, but the U.S. and UK governments have only formally attributed one of these sets—known as BERSERK BEAR—to FSB.

- **BERSERK BEAR (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope)** has, according to industry reporting, historically targeted entities in Western Europe and North America, including state, local, tribal, and territorial (SLTT) organizations, as well as Energy, Transportation Systems, and Defense Industrial Base (DIB) Sector organizations. This group has also targeted the Water and Wastewater Systems Sector and other critical infrastructure facilities. Common TTPs include scanning to exploit internet-facing infrastructure and network appliances, conducting brute force attacks against public-facing web applications, and leveraging compromised infrastructure—often websites frequented or

owned by their target—for Windows New Technology Local Area Network Manager (NTLM) credential theft. Industry reporting assesses that this actor has a destructive mandate.

The U.S. and UK governments assess that this APT group is almost certainly FSB's Center 16, or Military Unit 71330, and that FSB's Center 16 has conducted cyber operations against critical IT systems and infrastructure in Europe, the Americas, and Asia.

**Resources:** for more information on BERSERK BEAR, see the MITRE ATT&CK® webpage on Dragonfly.

**High-Profile Activity:** in 2017, FSB employees, including one employee in the FSB Center for Information Security (also known as Unit 64829 and Center 18), were indicted by the U.S. Department of Justice (DOJ) for accessing email accounts of U.S. government and military personnel, private organizations, and cybersecurity companies, as well as email accounts of journalists critical of the Russian government.[9] More recently, in 2021, FSB Center 16 officers were indicted by the U.S. DOJ for their involvement in a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data. One of the victims was a U.S. nuclear power plant.[10]

**Resources**: for more information on FSB, see:

- U.S. DOJ Press Release Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- UK Press Release UK Exposes Russian Spy Agency Behind Cyber Incidents

### *Russian Foreign Intelligence Service*

**Overview:** SVR has operated an APT group since at least 2008 that has targeted multiple critical infrastructure organizations. SVR cyber threat actors have used a range of initial exploitation techniques that vary in sophistication coupled with stealthy intrusion tradecraft within compromised networks. SVR cyber actors' novel tooling and techniques include:

- Custom, sophisticated multi-platform malware targeting Windows and Linux systems (e.g., GoldMax and TrailBlazer); and
- Lateral movement via the "credential hopping" technique, which includes browser cookie theft to bypass multifactor authentication (MFA) on privileged cloud accounts.[11]

**High-Profile Activity:** the U.S. Government, the Government of Canada, and the UK Government assess that SVR cyber threat actors were responsible for the SolarWinds Orion supply chain compromise and the associated campaign that affected U.S. government agencies, critical infrastructure entities, and private sector organizations.[12][13][14]

**Also known as:** APT29, COZY BEAR, CozyDuke, Dark Halo, The Dukes, NOBELIUM, and NobleBaron, StellarParticle, UNC2452, YTTRIUM [15]

**Resources**: for more information on SVR, see:

- Joint CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint Advisory Further TTPs associated with SVR cyber actors
- The MITRE ATT&CK webpage on APT29

For more information on the SolarWinds Orion supply chain compromise, see:

- CISA's Supply Chain Compromise webpage
- CISA's webpage on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- NCSC-UK Guidance Dealing with the SolarWinds Orion compromise

### *GRU, 85th Main Special Service Center*

**Overview:** GTsSS, or Unit 26165, is an APT group that has operated since at least 2004 and primarily targets government organizations, travel and hospitality entities, research institutions, and non-governmental organizations, in addition to other critical infrastructure organizations.

According to industry reporting, GTsSS cyber actors frequently collect credentials to gain initial access to target organizations. GTsSS actors have collected victim credentials by sending spearphishing emails that appear to be legitimate security alerts from the victim's email provider and include hyperlinks leading to spoofed popular webmail services' logon pages. GTsSS actors have also registered domains to conduct credential harvesting operations. These domains mimic popular international social media platforms and masquerade as tourism- and sports-related entities and music and video streaming services.

**High-Profile Activity:** the U.S. Government assesses that GTsSS cyber actors have deployed Drovorub malware against victim devices as part of their cyber espionage operations.[16] The U.S. Government and UK Government assess that GTsSS actors used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.[17]

**Also known as:** APT28, FANCY BEAR, Group 74, IRON TWILIGHT, PawnStorm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, Swallowtail, TG-4127, Threat Group-4127, and Tsar Team [18]

**Resources:** for more information on GTsSS, see the MITRE ATT&CK webpage on APT28.

### *GRU's Main Center of Special Technologies*

**Overview**: GTsST, or Unit 74455, is an APT group that has operated since at least 2009 and has targeted a variety of critical infrastructure organizations, including those in the Energy, Transportation Systems, and Financial Services Sectors. According to industry reporting, GTsST also has an extensive history of conducting cyber espionage as well as destructive and disruptive operations

against NATO member states, Western government and military organizations, and critical infrastructure-related organizations, including in the Energy Sector.

The primary distinguishing characteristic of the group is its operations use techniques aimed at causing disruptive or destructive effects at targeted organizations using DDoS attacks or wiper malware. The group's destructive operations have also leveraged wiper malware that mimics ransomware or hacktivism and can result in collateral effects to organizations beyond the primary intended targets. Some of their disruptive operations have shown disregard or ignorance of potential secondary or tertiary effects.

**High-Profile Activity:** the malicious activity below has been previously attributed to GTsST by the U.S. Government and the UK Government.[19][20]

- GTsST actors conducted a cyberattack against Ukrainian energy distribution companies in December 2015, leading to disruption of multiple companies' operations and widespread temporary outages. The actors deployed BlackEnergy malware to steal user credentials and used BlackEnergy's destructive component, KillDisk, to make infected computers inoperable.
- In 2016, GTsST actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware (also known as Industroyer) specifically designed to attack power grids.
- In June 2017, GTsST actors deployed NotPetya disruptive malware against Ukrainian financial, energy, and government organizations. NotPetya masqueraded as ransomware, had a large collateral impact, and caused damage to millions of devices globally.
- In 2018, GTsST actors deployed data-deletion malware against the Winter Olympics and Paralympics using VPNFilter.

The U.S. Government, Government of Canada, and UK Government have also attributed the October 2019 large-scale, disruptive cyber operations against a range of Georgian web hosting providers to GTsST. This activity resulted in websites—including sites belonging to the Georgian government, courts, non-government organizations (NGOs), media, and businesses—being defaced and interrupted the service of several national broadcasters.[21][22][23]

**Also known as:** ELECTRUM, IRON VIKING, Quedagh, the Sandworm Team, Telebots, VOODOO BEAR [24]

**Resources:** for more information on GTsST, see the MITRE ATT&CK webpage on Sandworm Team.

### *Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics*

**Overview:** TsNIIKhM, as described on their webpage, is a research organization under Russia's Ministry of Defense (MOD). Actors associated with TsNIIKhM have developed destructive ICS malware.

**High-Profile Activity:** TsNIIKhM has been sanctioned by the U.S. Department of the Treasury for connections to the destructive Triton malware (also called HatMan and TRISIS); TsNIIKhM has been sanctioned by the UK Foreign, Commonwealth, and Development Office (FCDO) for a 2017 incident

that involved safety override controls (with Triton malware) in a foreign oil refinery.[25][26] In 2021, the U.S. DOJ indicted a TsNIIKhM Applied Development Center (ADC) employee for conducting computer intrusions against U.S. Energy Sector organizations. The indicted employee also accessed the systems of a foreign oil refinery and deployed Triton malware.[27] Triton is a custom-built malware designed to manipulate safety instrumented systems within ICS controllers, disabling the safety alarms that prevent dangerous conditions.

**Also known as:** Temp.Veles, XENOTIME [28]

**Resources:** for more information on TsNIIKhM, see the MITRE ATT&CK webpage on TEMP.Veles. For more information on Triton, see:

- CISA Malware Analysis Report (MAR) HatMan – Safety System Targeted Malware (update B)
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- NCSC-UK Advisory TRITON Malware Targeting Safety Controllers

## Russian-Aligned Cyber Threat Groups

In addition to the APT groups identified in the Russian State-Sponsored Cyber Operations section, industry reporting identifies two intrusion sets—PRIMITIVE BEAR and VENOMOUS BEAR—as state-sponsored APT groups, but U.S., Australian, Canadian, New Zealand, and UK cyber authorities have not attributed these groups to the Russian government.

- **PRIMITIVE BEAR** has, according to industry reporting, targeted Ukrainian organizations since at least 2013. This activity includes targeting Ukrainian government, military, and law enforcement entities using high-volume spearphishing campaigns to deliver its custom malware. According to industry reporting, PRIMITIVE BEAR conducted multiple cyber operations targeting Ukrainian organizations in the lead up to Russia's invasion.

  **Resources:** for more information on PRIMITIVE BEAR, see the MITRE ATT&CK webpage on the Gamaredon Group.

- **VENOMOUS BEAR** has, according to industry reporting, historically targeted governments aligned with the North Atlantic Treaty Organization (NATO), defense contractors, and other organizations of intelligence value. Venomous Bear is known for its unique use of hijacked satellite internet connections for command and control (C2). It is also known for the hijacking of other non-Russian state-sponsored APT actor infrastructure.[29] VENOMOUS BEAR has also historically leveraged compromised infrastructure and maintained an arsenal of custom-developed sophisticated malware families, which is extremely complex and interoperable with variants developed over time. VENOMOUS BEAR has developed tools for multiple platforms, including Windows, Mac, and Linux.[30]

  **Resources:** for more information on VENOMOUS BEAR, see the MITRE ATT&CK webpage on Turla.

## Russian-Aligned Cybercrime Groups

Cybercrime groups are typically financially motivated cyber actors that seek to exploit human or security vulnerabilities to enable direct theft of money (e.g., by obtaining bank login information) or by extorting money from victims. These groups pose consistent threats to critical infrastructure organizations globally.

Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine. These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations primarily through:

- Deploying ransomware through which cyber actors remove victim access to data (usually via encryption), potentially causing significant disruption to operations.
- Conducting DDoS attacks against websites.
    - In a DDoS attack, the cyber actor generates enough requests to flood and overload the target page and stop it from responding.
    - DDoS attacks are often accompanied by extortion.
    - According to industry reporting, some cybercrime groups have recently carried out DDoS attacks against Ukrainian defense organizations, and one group claimed credit for DDoS attack against a U.S. airport the actors perceived as supporting Ukraine (see the Killnet section).

Based on industry and open-source reporting, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess multiple Russian-aligned cybercrime groups pose a threat to critical infrastructure organizations. These groups include:

- **The CoomingProject**
- **Killnet**
- **MUMMY SPIDER**
- **SALTY SPIDER**
- **SCULLY SPIDER**
- **SMOKEY SPIDER**
- **WIZARD SPIDER**
- **The Xaknet Team**

**Note:** although some cybercrime groups may conduct cyber operations in support of the Russian government, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess that cyber criminals will most likely continue to operate primarily based on financial motivations, which may include targeting government and critical infrastructure organizations.

### *The CoomingProject*

**Overview:** the CoomingProject is a criminal group that extorts money from victims by exposing or threatening to expose leaked data. Their data leak site was launched in August 2021.[31] The

CoomingProject stated they would support the Russian Government in response to perceived cyberattacks against Russia.[32]

### *Killnet*

**Overview:** according to open-source reporting, Killnet released a video pledging support to Russia.[33]

**Victims:** Killnet claimed credit for carrying out a DDoS attack against a U.S. airport in March 2022 in response to U.S. materiel support for Ukraine.[34]

### *MUMMY SPIDER*

**Overview**: MUMMY SPIDER is a cybercrime group that creates, distributes, and operates the Emotet botnet. Emotet is advanced, modular malware that originated as a banking trojan (malware designed to steal information from banking systems but that may also be used to drop additional malware and ransomware). Today Emotet primarily functions as a downloader and distribution service for other cybercrime groups. Emotet has been used to deploy WIZARD SPIDER's TrickBot, which is often a precursor to ransomware delivery. Emotet has worm-like features that enable rapid spreading in an infected network.

**Victims:** according to open sources, Emotet has been used to target industries worldwide, including financial, e-commerce, healthcare, academia, government, and technology organizations' networks.

**Also known as:** Gold Crestwood, TA542, TEMP.Mixmaster, UNC3443

**Resources:** for more information on Emotet, see joint Alert Emotet Malware. For more information on TrickBot, see joint CSA TrickBot Malware.

### *SALTY SPIDER*

**Overview:** SALTY SPIDER is a cybercrime group that develops and operates the Sality botnet. Sality is a polymorphic file infector that was discovered in 2003; since then, it has been replaced by more advanced peer-to-peer (P2P) malware loaders.[35]

**Victims:** according to industry reporting, in February 2022, SALTY SPIDER conducted DDoS attacks against Ukrainian web forums used to discuss events relating to Russia's military offensive against the city of Kharkiv.

**Also known as:** Sality

### *SCULLY SPIDER*

**Overview:** SCULLY SPIDER is a cybercrime group that operates using a malware-as-a-service model; SCULLY SPIDER maintains command and control infrastructure and sells access to their malware and infrastructure to affiliates, who distribute their own malware.[36][37] SCULLY SPIDER develops and operates the DanaBot botnet, which originated primarily as a banking Trojan but expanded beyond banking in 2021 and has since been used to facilitate access for other types of malware, including TrickBot, DoppelDridex, and Zloader. Like Emotet, Danabot effectively functions as an initial access vector for other malware, which can result in ransomware deployment.

According to industry reporting, recent DDoS activity by the DanaBot botnet suggests SCULLY SPIDER has operated in support of Russia's military offensive in Ukraine.

**Victims:** SCULLY SPIDER affiliates have primarily targeted organizations in the United States, Canada, Germany, United Kingdom, Australia, Italy, Poland, Mexico, and Ukraine.[38] According to industry reporting, in March 2022, Danabot was used in DDoS attacks against multiple Ukrainian government organizations.

**Also known as:** Gold Opera

### *SMOKEY SPIDER*

**Overview:** SMOKEY SPIDER is a cybercrime group that develops Smoke Loader (also known as Smoke Bot), a malicious bot that is used to upload other malware. Smoke Loader has been available since at least 2011, and operates as a malware distribution service for a number of different payloads, including—but not limited to—DanaBot, TrickBot, and Qakbot.

**Victims:** according to industry reporting, Smoke Loader was observed in March 2022 distributing DanaBot payloads that were subsequently used in DDoS attacks against Ukrainian targets.

**Resources:** for more information on Smoke Loader, see the MITRE ATT&CK webpage on Smoke Loader.

### *WIZARD SPIDER*

**Overview:** WIZARD SPIDER is a cybercrime group that develops TrickBot malware and Conti ransomware. Historically, the group has paid a wage to the ransomware deployers (referred to as affiliates), some of whom may then receive a share of the proceeds from a successful ransomware attack. In addition to TrickBot, notable initial access and persistence vectors for affiliated actors include Emotet, Cobalt Strike, spearphishing, and stolen or weak Remote Desktop Protocol (RDP) credentials.

After obtaining access, WIZARD SPIDER affiliated actors have relied on various publicly available and otherwise legitimate tools to facilitate earlier stages of the attack lifecycle before deploying Conti ransomware.

WIZARD SPIDER pledged support to the Russian government and threatened critical infrastructure organizations of countries perceived to carry out cyberattacks or war against the Russian government.[39] They later revised this pledge and threatened to retaliate against perceived attacks against the Russian people.[40]

**Victims:** Conti victim organizations span across multiple industries, including construction and engineering, legal and professional services, manufacturing, and retail. In addition, WIZARD SPIDER affiliates have deployed Conti ransomware against U.S. healthcare and first responder networks.

**Also known as:** UNC2727, Gold Ulrick

**Resources:** for more information on Conti, see joint CSA Conti Ransomware. For more information on TrickBot, see joint CSA TrickBot Malware.

### *The XakNet Team*

**Overview:** XakNet is a Russian-language cyber group that has been active as early as March 2022. According to open-source reporting, the XakNet Team threatened to target Ukrainian organizations in response to perceived DDoS or other attacks against Russia.[41] According to reporting from industry, on March 31, 2022, XakNet released a statement stating they would work "exclusively for the good of [Russia]." According to industry reporting, the XakNet Team may be working with or associated with Killnet actors, who claimed credit for the DDoS attacks against a U.S. airport (see the Killnet section).

**Victims:** according to industry reporting, in late March 2022, the XakNet Team leaked email contents of a Ukrainian government official. The leak was accompanied by a political statement criticizing the Ukrainian government, suggesting the leak was politically motivated.

## MITIGATIONS

U.S., Australian, Canadian, New Zealand, and UK cyber authorities urge critical infrastructure organizations to prepare for and mitigate potential cyber threats by immediately (1) updating software, (2) enforcing MFA, (3) securing and monitoring RDP and other potentially risky services, and (4) providing end-user awareness and training.

- **Update software, including operating systems, applications, and firmware, on IT network assets.** Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
    - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
    - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.
- **Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords**. Do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. As Russian state-sponsored APT actors have demonstrated the ability to exploit default MFA protocols and known vulnerabilities, organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios. For more information, see joint CSA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability.
- **If you use RDP and/or other potentially risky services, secure and monitor them closely.** RDP exploitation is one of the top initial infection vectors for ransomware, and risky

services, including RDP, can allow unauthorized access to your session using an on-path attacker.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN) or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force attempts, log RDP login attempts, and disable unused remote access/RDP ports.
    - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).

- **Provide end-user awareness and training** to help prevent successful targeted social engineering and spearphishing campaigns. Phishing is one of the top infection vectors for ransomware, and Russian state-sponsored APT actors have conducted successful spearphishing campaigns to gain credentials of target networks.
    - Ensure that employees are aware of potential cyber threats and delivery methods.
    - Ensure that employees are aware of what to do and whom to contact when they receive a suspected phishing email or suspect a cyber incident.

As part of a longer-term effort, **implement network segmentation to separate network segments based on role and functionality**. Network segmentation can help prevent the spread of ransomware and threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Ensure OT assets are not externally accessible. Ensure strong identity and access management when OT assets needs to be externally accessible.
- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by considering criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

To further prepare for and mitigate cyber threats from Russian state-sponsored or criminal actors, U.S., Australian, Canadian, New Zealand, and UK cyber authorities encourage critical infrastructure organizations to implement the recommendations listed below.

## Preparing for Cyber Incidents

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
  - Ensure the cyber incident response plan contains ransomware- and DDoS-specific annexes. For information on preparing for DDoS attacks, see NCSC-UK guidance on preparing for denial-of-service attacks.
  - Keep hard copies of the incident response plan to ensure responders and network defenders can access the plan if the network has been shut down by ransomware, etc.
- Maintain offline (i.e., physically disconnected) backups of data. Backup procedures should be conducted on a frequent, regular basis (at a minimum every 90 days). Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.
  - Ensure the backup keys are kept offline as well, to prevent them being encrypted in a ransomware incident.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure with a particular focus on key data assets.
- Develop recovery documentation that includes configuration settings for common devices and critical equipment. Such documentation can enable more efficient recovery following an incident.
- Identify the attack surface by mapping and accounting all external-facing assets (applications, servers, IP addresses) that are vulnerable to DDoS attacks or other cyber operations.
- For OT assets/networks:
  - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
  - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated from IT networks if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety-critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
  - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
  - Implement data backup procedures.
  - Develop recovery documents that include configuration settings for common devices and critical OT equipment.

## Identity and Access Management

- Require accounts with password logins, including service accounts, to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. Consider using a password manager; see NCSC-UK's Password Manager Buyers Guide for guidance.

- Implement authentication timeout and lockout features to prevent repeated failed login attempts and successful brute-force attempts.
- Create a deny list of known compromised credentials and prevent users from using known-compromised passwords.
- Secure credentials by restricting where accounts and credentials can be used and by using local device credential protection features. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
    - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
    - Ensure storage of clear text passwords in Local Security Authority Subsystem Service (LSASS) memory is disabled. **Note:** for Windows 8, this is enabled by default. For more information see Microsoft Security Advisory Update to Improve Credentials Protection and Management.
    - Consider disabling or limiting NTLM and WDigest Authentication.
    - Implement Credential Guard for Windows 10 and Server 2016 (refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
    - Minimize the Active Directory (AD) attack surface to reduce malicious ticket-granting activity. Malicious activity such as “Kerberoasting” takes advantage of Kerberos’ Ticket Granting Service (TGS) and can be used to obtain hashed credentials that malicious cyber actors attempt to crack.
- Audit domain controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
    - Secure accounts.
    - Enforce the principle of least privilege. Administrator accounts should have the minimum permission necessary to complete their tasks.
    - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
    - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- Disable inactive accounts uniformly across the AD, MFA systems, etc.
- Implement time-based access for privileged accounts. The FBI and CISA observed cybercriminals conducting increasingly impactful attacks against U.S. entities on holidays and weekends in 2021. Threat actors may view holidays and weekends—when offices are normally closed—as attractive timeframes, as there are fewer network defenders and IT support personnel at victim organizations. The just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the zero-trust model) by setting network-wide policy to automatically disable admin accounts at the AD level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe.

## Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor, ransomware, or other malware. Use network monitoring tools and host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Implement a firewall and configure it to block Domain Name System (DNS) responses from outside the enterprise network or drop Internet Control Message Protocol (ICMP) packets. Review which admin services need to be accessible externally and allow those explicitly, blocking all others by default.
    - U.S. Defense Industrial Base organizations may sign up for the NSA Cybersecurity Collaboration Center's Protective Domain Name System (PDNS) services.
- Enable web application firewalls to mitigate application-level DDoS attacks.
- Implement a multi-content delivery network (CDN) solution. This will minimize the threat of DDoS attacks by distributing and balancing web traffic across a network.

## Vulnerability and Configuration Management

- Use an antivirus programs that uses heuristics and reputational ratings to check a file's prevalence and digital signature prior to execution. **Note**: organizations should assess the risks inherent in their software supply chain (including its security/antivirus software supply chain) in light of the existing threat landscape.
    - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
    - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.
- Disable all unnecessary ports and protocols.
    - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control activity.
    - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Identify business-to-business VPNs and block high-risk protocols.
- Ensure OT hardware is in read-only mode.
- Enable strong spam filters.
    - Enable strong spam filters to prevent phishing emails from reaching end users.
    - Filter emails containing executable files to prevent them from reaching end users.

- Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.

- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Open document readers in protected viewing modes to help prevent active content from running.

## Responding to Cyber Incidents

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge network defenders of critical infrastructure organizations to exercise due diligence in identifying indicators of malicious activity. Organizations detecting potential APT or ransomware activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. For DDoS attacks:
    a. Identify the source address originating the attack via the SIEM or logging service. If the attack is originating from a single pool of IP addresses, block IP traffic from suspected IPs via access control lists or by contacting your internet service provider (ISP).
    b. Enable firewall rate limiting to restrict the amount of IP traffic coming in from suspected IP addresses
    c. Notify your ISP and enable remote triggered blackhole (RTBH).
3. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
4. Collect and review relevant logs, data, and artifacts.
5. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
6. Report incidents to appropriate cyber and law enforcement authorities:
    - **U.S organizations:** share information about incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 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. For ransomware incidents, organizations can also report to the U.S. Secret Service via a U.S. Secret Service Field Office.

- **Australian organizations:** if you have questions about this advice or have indications that your environment has been compromised, call the ACSC at 1300 CYBER1 (1300 292 371). To report an incident see cyber.gov.au/acsc/report.
- **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca.
- **New Zealand organizations**: if your organization requires assistance from the National Cyber Security Centre, contact them directly via telephone at (04) 498-7654 or via email at ncscincidents@ncsc.govt.nz.
- **UK organizations:** report a significant cybersecurity incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

For additional guidance on responding to a ransomware incident, see the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on hunting or investigating a network, and for common mistakes in incident handling.

Additionally, CISA, the FBI, and NSA encourage U.S. critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

**Note:** U.S., Australian, Canadian, New Zealand, and UK cyber authorities strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom does not guarantee that a victim's files will be recovered.

## RESOURCES

- For more general information on Russian state-sponsored malicious cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage and joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.
- For alerts on malicious and criminal cyber activity, see the FBI Internet Crime Complaint Center webpage.
- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. government webpage providing ransomware resources and alerts.
- For more information on mitigating DDoS attacks, see NCSC-UK Denial of Service (DoS) Guidance.

- For more information on managing cybersecurity incidents, see NZ NCSC Incident Management: Be Resilient, Be Prepared.
- For information on destructive malware, see joint CSA Destructive Malware Targeting Organizations in Ukraine.
- Critical infrastructure owners and operators with OT/ICS networks should review the following resources for additional information:
    - Joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
    - CISA factsheet Rising Ransomware Threat to Operational Technology Assets

## DISCLAIMER

The information you have accessed or received is being provided "as is" for informational purposes only. CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, and the UK National Crime Agency (NCA) do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.

## TRADEMARK RECOGNITION

MITRE and ATT&CK are registered trademarks of The MITRE Corporation. Kubernetes is a registered trademark of The Linux Foundation.

## PURPOSE

This document was developed by U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

## REFERENCES

[1] Cybersecurity and Infrastructure Security Agency

[2] Federal Bureau of Investigation

[3] National Security Agency

[4] Australian Cyber Security Centre

[5] Canadian Centre for Cyber Security

[6] New Zealand's National Cyber Security Centre

[7] United Kingdom's National Cyber Security Centre

[8] United Kingdom's National Crime Agency

[9] U.S. DOJ Press Release: U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts

[10] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide

[11] CrowdStrike Blog: Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign

[12] U.S. White House Statement: FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government

[13] Government of Canada Statement on SolarWinds Cyber Compromise

[14] UK Government Press Release: Russia: UK and US expose global campaign of malign activity by Russian intelligence services

[15] MITRE ATT&CK: APT29

[16] Joint CSA Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware

[17] Joint CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

[18] MITRE ATT&CK APT28

[19] Joint CSA New Sandworm Malware Cyclops Blink Replaces VPNFilter

[20] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks

[21] U.S. Department of State, Press Statement: The United States Condemns Russian Cyber Attack Against the Country of Georgia

[22] Government of Canada CSE Statement on Malicious Russian Cyber Activity Targeting Georgia

[23] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks

[24] MITRE ATT&CK The Sandworm Team

[25] U.S. Department of the Treasury Press Release: Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware

[26] UK Government Press Release: UK exposes Russian spy agency behind cyber incident.

[27] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide

[28] MITRE ATT&CK TEMP.Veles

[29] NSA and NCSC-UK Cybersecurity Advisory Turla Group Exploits Iranian APT To Expand Coverage Of Victims

[30] CrowdStrike Adversary Profile: VENEMOUS BEAR

[31] KELA Cybersecurity Intelligence Center: Ain't No Actor Trustworthy Enough: The importance of validating sources

[32] Twitter: Valery Marchive Status, Feb. 25, 2022 1:41 PM

[33] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides

[34] Twitter: CyberKnow Status, March 29, 2022, 7:54 AM

[35] CrowdStrike Blog: Who is Salty Spider (Sality)?

[36] Proofpoint Blog: New Year, New Version of DanaBot

[37] Zscaler Blog: Spike in DanaBot Malware Activity

[38] Proofpoint Blog: New Year, New Version of DanaBot

[39] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides.

[40] TechTarget: Conti ransomware gang backs Russia, threatens US

[41] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides

## ACKNOWLEDGEMENTS

The U.S., Australian, Canadian, New Zealand, and UK cyber authorities would like to thank CrowdStrike, Google, LookingGlass Cyber, Mandiant, Microsoft, and Secureworks for their contributions to this CSA.