Joint Statement on the International Counter Ransomware Initiative

November 1, 2022

The members of the International Counter Ransomware Initiative (CRI)—Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Poland, Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine, and the European Union—met in Washington, DC on October 31–November 1, 2022. Previously participating states welcome Belgium as a new CRI member.

At the Second CRI Summit, members re-affirmed our joint commitment to building our collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat.

The work of the CRI supports the implementation of the endorsed UN framework for responsible state behavior in cyberspace, specifically the voluntary norm that States should cooperate "to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats." The joint efforts of the CRI partners are also directly contributing to the implementation of the consensus conclusions and recommendations of the UN Expert Group to Conduct a Comprehensive Study on Cybercrime.

We are committed to using all appropriate tools of national power to achieve these goals and jointly committed to the following actions in support of this endeavor. We intend to:

- Hold ransomware actors accountable for their crimes and not provide them safe haven;
- Combat ransomware actors' ability to profit from illicit proceeds by implementing and enforcing anti–money laundering and countering the financing of terrorism (AML/CFT) measures, including "know your customer" (KYC) rules, for virtual assets and virtual asset service providers;
- Disrupt and bring to justice ransomware actors and their enablers, to the fullest extent permitted under each partner's applicable laws and relevant authorities; and
- Collaborate in disrupting ransomware by sharing information, where appropriate and in line with applicable laws and regulations, about the misuse of infrastructure to launch ransomware attacks to ensure national cyber infrastructure is not being used in ransomware attacks.

Building our resilience to ransomware attacks requires effective policies and cooperation with trusted partners. CRI members are building a network of trusted partners to share and disseminate ransomware-related threat information to increase our collective resilience to ransomware attacks. To that end, we intend to establish a voluntary International Counter Ransomware Task Force (ICRTF) to develop cross-sectoral tools and cyber threat intelligence exchange to increase early warning capabilities and prevent attacks, as well as consolidate policy and best practice frameworks. The ICRTF expects to produce public reports on tools, tactics, and procedures to improve awareness to global stakeholders, promote and encourage membership of the CRI, and improve cyber hygiene across the board. The ICRTF intends to consider a model for

ongoing collaboration with key private sector partners, including the establishment of an ancillary industry chapter that would be actively engaged with the work of the ICRTF.

We commit to establish processes to most effectively share information and analysis about specific strains of ransomware on an ongoing and enduring basis to improve our collective awareness and resilience.

CRI members are committed to taking action, in line with national law and policy, to disrupt and degrade the ransomware ecosystem and hold accountable criminal ransomware actors based on our collective knowledge, expertise, authorities, and capabilities. We intend to improve our comprehensive and holistic understanding of the strategies used by these criminal actors and the means by which their malicious activity can be identified and addressed in respective jurisdictions to improve our tools, relevant authorities, and capabilities to disrupt. We commit to work together to prioritize disruption targets to leverage the breadth of authorities and tools available to pursue hard and complex targets more effectively. We intend to increase the number and impact of our disruption actions so that ransomware actors are stopped in their tracks.

The CRI is committed not only to protecting ourselves and each other from ransomware, but also to helping other countries protect and disrupt so that ransomware is unable to gain traction worldwide. To that end, we intend to share technical and threat information and provide protection and remediation recommendations as broadly as possible.

Taking decisive steps to counter illicit finance that often enables and underpins the profitability of ransomware will also be key to our collective success. We resolve to work to establish mechanisms for notifying financial institutions and virtual asset platforms of ransomware payments so that funds can potentially be seized once they land in ransomware actors' accounts. We commit to working together to promote AML/CFT controls, including KYC policies and procedures within the virtual assets ecosystem to prevent its use for ransomware activity, such as through the implementation and enforcement of the Financial Action Task Force recommendations.

The private sector has a unique role to play in our counter-ransomware efforts, as their insights into the whereabouts and actions of ransomware actors from across the internet can effectively complement state capabilities in this realm. Private sector companies are often the victims of ransomware, and can be strong allies in defense and disruption. CRI members are working closely with the private sector to share information and set goals to prevent, reduce, and respond to ransomware threats. To further this collaboration, we have established a pilot information sharing platform to facilitate the exchange of information about ransomware actors and tools, tactics, techniques, and procedures amongst members, and eventually with the private sector. In addition, we also intend to develop a capacity-building tool to help countries utilize public-private partnerships to combat ransomware. We are continuing to work together to develop additional ways to collaborate to combat ransomware with the private sector, taking into account concerns private sector companies may raise.

Diplomatic engagement continues to be an essential tool for the international community's fight against ransomware attacks. We are committed to continuing to work together not only as the CRI, but also with other partners committed to fighting the scourge of ransomware, which has the power to impact us all, including through the Paris Call for Trust and Security for CRI members that support the Call. CRI members plan to work with the full spectrum of stakeholders to drive focused regional efforts and advance this agenda in appropriate multilateral frameworks to ensure the global community's shared resolve and preparedness to defeat these threats. We are also committed to leveraging capacity building programs in order to strengthen resilience, improve disruption capabilities, increase law enforcement capacities, and support the development of legal frameworks to combat ransomware in both CRI and other countries. In this

regard, we intend to conduct bi-annual cyber exercises for the CRI Member States, which will also contribute to living toolkit of the ICRTF.

NOTE: An original was not available for verification of the content of this joint statement.

Categories: Joint Statements : International Counter Ransomware Initiative.

Subjects: Counter Ransomware Initiative, International; Defense and national security : Cybersecurity :: Cyber attacks; Defense and national security : Cybersecurity :: Strengthening efforts.

DCPD Number: DCPD202200990.