RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 166 – 15 November 2021

US Global Ransomware Summit: More Needs to be Done

By Gil Baram

SYNOPSIS

The US Justice Department's arrest of several affiliates of the Russian-speaking REvil ransomware group comes a month after Washington hosted a virtual international summit on ransomware attacks. The decision to leave Russia out of the summit will inevitably limit the effectiveness of the operation.

COMMENTARY

ON 8 NOVEMBER 2021, the US Justice Department announced the arrest of several members of the Russian-speaking REvil ransomware group, in a large-scale operation involving US allies in Europe and around the globe. The REvil group, who have since been charged, have been deploying ransomware attacks against American targets including the software provider Kaseya in July 2021. Furthermore, the State Department added REvil to a bounty programme that offers up to US$10 million for information on the REvil leaders.

These efforts followed the two-day virtual international summit on ransomware hosted by the Biden administration on 13-14 October. This summit included 30 countries and was a decisive step towards building a coalition against ransomware attacks. It was acknowledged by all countries that ransomware posed a global and national security threat. Russia ─ as well as China, Iran, and North Korea ─ was not invited.

From Petty Crime to Global Criminal Enterprises

The summit prompted some governments to state their positions on state-sponsored ransomware. Australia, the Netherlands and United Kingdom began signalling a more aggressive, military, and intelligence agency-backed response to the ransomware threat.

Lindy Cameron, head of the British National Cyber Security Centre (NCSC) said: “In addition to the direct cyber security threats that the Russian state poses, we […] assess that cyber criminals based in Russia and neighbouring countries are responsible for most of the devastating ransomware attacks against UK targets.”

On average there is a new ransomware attack every 11 seconds, and the losses to organisations from ransomware attacks are projected to reach $20 billion over the course of 2021. According to the White House, ransomware payments rose to more than $400 million globally last year.

COVID-19 increased these numbers, as many organisations started operating remotely, making themselves even more vulnerable. In fact, ransomware has existed for several decades and is therefore not new. The problem has been regarded for a long time as "e-crime", which primarily affects the private sector, and was not viewed as a security issue.

The ransomware threat has, however, evolved from a “petty crime to a major economic windfall for global criminal enterprises”. The rise of cryptocurrencies makes it difficult for funds to be traced as these can be transferred electronically without the assistance of other institutions regulated by governments. This has contributed to the rise of ransomware attacks.

Global Cooperation on Cyber Issues: Limited Success

The growing international attention on ransomware and its treatment as a national security threat have changed how countries respond to this new challenge. However, global cooperation on cyber issues has so far achieved limited success because of two reasons: Firstly, it has been done without the cooperation of Russia and China. Secondly, deterrence in cyberspace generally does not achieve its goal in the face of actors with different values and operating methods.

Past international efforts to promote global initiatives on agreed behaviour in cyberspace ─ like the UN GGE (Group of Governmental Experts) ─ suffered from disagreements among the nation-states. The main ones are largely between the US and Russia as well as China regarding the meaning of sovereignty in cyberspace and its implications for improving global cyber stability.

This year, the UN GGE had reached agreements while the UN Open-Ended Working Group (OEWG) achieved some non-binding understandings on ways to advance peace and security in cyberspace. The OEWG includes representatives from multiple countries and stakeholders.

An international summit that did not include Russia and China (among others) is unlikely to lead to actionable results that reduce the severity and intensity of global ransomware attacks. In May 2021 President Biden warned Moscow about the need to “take decisive action” against them. The Justice Department, he said, would step up prosecutions of ransomware hackers and the government will “pursue a measure to disrupt their ability to operate”.

Russia’s Lack of Action

Despite this warning, there has been little or no change in the Russian stance that would indicate Moscow's acceptance of the presence of ransomware attacks by Russia-affiliated criminal groups. And despite repeated requests from the Biden administration, there is no evidence that Russia has taken action to deal with ransomware criminals operating within its borders and it is practically serving as a safe haven for cyber criminals.

The US has already sanctioned Russian individuals for committing cyberattacks but that did not seem to affect Russia's support for them.

Experts suggest that the US should act against cyber criminals the same way it acted against ISIS. Here the situation might pose some complications as these cyber criminals are operating within the borders of sovereign states.

But there might be some room for optimism from the latest round of strategic dialogue between the US and Russia that took place at the end of September. According to Russian news reports, Moscow and Washington have resumed some cooperation in cyber areas that have been frozen for many years.

Progress and Way Forward

There has been substantial progress reached in three key areas:

• At the end of September, The Kremlin and the White House resumed regular cybersecurity expert meetings.
• Both countries restored cooperation within the framework of the 1999 Mutual Legal Assistance in Criminal Cases Treaty. As a result, the US provided key information to enable the prosecution of several international cybercrime groups such as Evil Corp, REvil, and TrickBot. Specifically, Russia informed the US that it already started prosecuting hackers using malware from one of those three groups, and Moscow expressed willingness to continue collaborating on this track.
• The US and Russian cyber incident response centres also reestablished regular contacts and resumed information exchange on cyberattacks.

Going forward, the US ransomware summit was an important first step; it seems that many countries today perceive ransomware as a security threat and one that calls for a joint global action ─ as the recent operation and arrests show.

However, as long as Russia keeps providing safe haven for cyber criminals this activity will not be resolved. The US should reach out to Russia as well as other nations and lead international effort in a more inclusive way if it wants to reach a global and long-lasting solution.

Gil Baram is a Fulbright Cybersecurity post-doctoral fellow, Center for International Security and Cooperation (CISAC) Stanford University, and an Adjunct Research Fellow at the Centre of Excellence for National Security, (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg