G7 calls on Russia to crack down on ransomware gangs

R. therecord.media/g7-calls-on-russia-to-crack-down-on-ransomware-gangs/

In light of the recent wave of high-profile ransomware attacks that have caused havoc in the US and Europe, the member states of the G7 group have called on Russia and other countries to crack down on ransomware gangs operating within their borders.

"We call on all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions," the G7 group said in a communique [_PDF_] published on Sunday, at the end of a three-day conference held in Cornwall, UK.

"In particular, we call on Russia [...] to identify, disrupt, and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes," the G7 group added.

The joint statement was signed by the governments of Canada, France, Germany, Italy, Japan, the UK, and the US — more commonly known as the Group of Seven (G7).

It comes after a series of ransomware attacks that caused disruptions at hospitals during the COVID-19 pandemic, fuel outages on the US East Coast following the Colonial Pipeline attack, and beef supply issues across Australia and the US following the JBS Foods ransomware incident.

The aforementioned attacks brought the issue of ransomware from the depths of incident response reports to daily White House national security briefings, forcing the US and its fellow G7 members, who are facing similar rising waves of disruptive ransomware attacks, to take action on a global political level.

> At WH Press briefing, @JakeSullivan46 said the G7 Summit leaders will make commitments on ransomware at the upcoming summit.
>
> — Metacurity – The Cybersecurity News Curator (@Metacurity) June 7, 2021

It is unclear how yesterday's communique will contribute to the actual fight against ransomware gangs.

The vague statement yesterday, just urging other countries to fix their problems, with no actionable steps, has also been described as rhetoric.

> The g7 has agreed to tackle ransomware. So that's all sorted then, pack it up, we're done.
>
> — Barry Dorrans (@blowdart) June 13, 2021

> Great to see ransomware payments being raised at G7. I'd like to see some options of how organisations can be supported by government before we hail blocking payments as the solution. Too much talk of "fix backups and the problem is solved", it's never that simple.
>
> — Tom Hall (@thall_sec) June 12, 2021

Most ransomware gangs are believed to operate from within the borders of former Soviet states.

Most of these groups operate under unwritten rules that as long as they launch attacks exclusively against western countries and avoid Russia and its neighboring countries, they are left to operate in peace by local authorities.

Previously, US intelligence said that at least one cybercrime group's members (Evil Corp) operate under protection and in cooperation with Russia's internal intelligence service, the Federal Security Service (FSB).

Earlier today, Lindy Cameron, chief executive of the UK National Cyber Security Centre, called ransomware attacks the biggest online threat to UK users, far greater than nation-state hacking groups, highlighting that while state-sponsored groups might go after a limited number of targets and engage in silent espionage, ransomware gangs operate indiscriminately and have no reservations in causing large-scale disruptions in order to extract ransom payments.

Tags

- cybercrime
- G7
- Government
- politics
- Ransomware
- Russia

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.