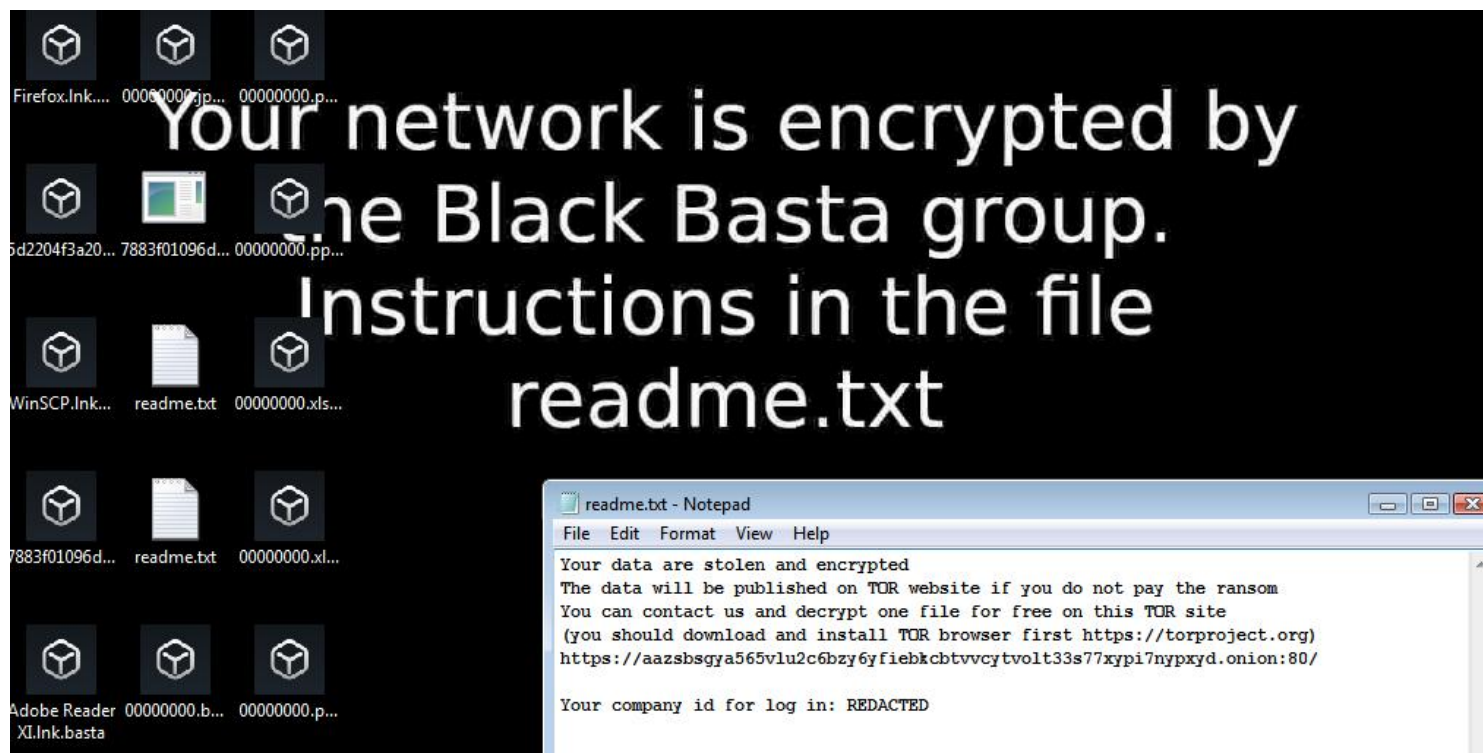


Weekly Intelligence Brief

A Chanticleer Intelligence Brief Project



Russian Linked Ransomware Group Leaked Chat Logs

Jordan Maple
Head of Desk
Cyber/Transnational Desk

On 11 FEB, internal chat logs of ransomware group Black Basta were leaked on Telegram, revealing over 200,000 messages from SEP 2023 to SEP 2024. Black Basta is a Russian-speaking criminal organization linked to cyber-attacks on American and British healthcare and infrastructure companies. This leak is connected to internal conflict between the group. Some possible reasons for this leak include reports of failure to provide ransomware as a service software to clients and claims of Black Basta planning to target Russian domestic banks.

The chat logs revealed techniques they used to target companies, including attacks on routers and firewalls that sit on the edge of the companies' networks. They were also in the process of targeting VPN networks by recruiting specialists who have experience in attacking these targets or by acquiring exploits. They were also known for using social engineering methods to send malicious files to victims. Cybersecurity firm Hudson Rock has launched an artificial intelligence platform known as BlackBastaGPT for threat intelligence researchers to comb through the 200,000 messages and provide a summarization of the logs.

The Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency have taken notice of Black Basta

with advisories from MAY 2024 warning potential victims of Black Basta's fraudulent schemes. Logs confirmed Black Basta members were concerned with repercussions from the two organizations. Members also expressed concerns that Russian authorities could consider investigating the group. These comments coincide with reports of high-ranking officials in Black Basta leaving the organization for Cactus Ransomware and other groups.

We can assess with high confidence it is unlikely Black Basta will continue operations due to the breaches and recent exodus of members. Additionally, we can assess with high confidence it is likely members of Black Basta will be investigated by American, British, or Russian authorities.

United States and Chinese Technology Companies Partner to Develop Quantum Computer Software

Ryan Campbell
Senior Analyst
Cyber/Transnational Desk

On 12 FEB, a U.S. based tech company named Phoenix, a decentralized artificial intelligence and decentralized physical infrastructure network (DePIN) compute network, has partnered with Origin Quantum, China's leading quantum computing firm. The partnership aims to build on Origin Quantum's most famous quantum system, known as "Origin Wukong."

Phoenix plans to leverage Origin's 72-qubit quantum chip to run just shy of Google's 105-qubit quantum chip, known

as Willow. They also plan to develop Quantum Virtual Machine (QuantumVM) which is expected to allow researchers and developers to create functions, perform calculations, and develop applications on the Origin quantum chip through a simplified web service API. This allows users to input commands without needing any understanding of quantum programming or circuits. Additionally, a web-based quantum computing terminal will be built on top of QuantumVM, allowing users to execute their previous functions and programs or any other calculation or program that has been uploaded with no prior knowledge or base code needed. These projects aim at making quantum computing cheaper for both the private and public sectors with

minimal upfront costs for the finished product and less required overall knowledge to operate.

We can assess with high confidence that it is highly likely that the release of QuantumVM will generate a more accessible quantum ecosystem for both the private and public cyber sector.



Mass protests in Serbia Increase Tensions in Balkans

Matthew Petersen
Senior Analyst
Europe Desk

On 15 FEB, tens of thousands of Serbian citizens flooded the streets of Kragujevac, Serbia, in support of student protests over a canopy collapse that left 15 dead in November. Since the collapse, students have demanded accountability from the Serbian government and transparency in the building codes for the canopy that collapsed. They have also called for action against those that retaliated and attempted to stop the protests and advocated for the release of protesters that were arrested.

Serbia's president, Aleksandar Vucic, issued statements claiming that these protests were sponsored by foreign actors and are a campaign meant to take him from power. These fears led to Vucic deporting five Croatian students in late January, claiming they were a threat to Serbian security after they were found to be protesting the response to the canopy collapse. Croatia has responded by issuing a warning to its citizens not to travel to Serbia unnecessarily.

Serbia has also denied entry and expelled students from Romania, Slovenia, Bosnia, and North Macedonia since the protests began in November. Vucic has also staged counter protests and rallies in support of the current administration, where he condemned

the current protests and alluded that the only way he will step down is if he is killed. These protests in Serbia have spilled over into the surrounding countries, inspiring Bosnian citizens to demand accountability for the government's response to flooding in October. Countries such as Bulgaria, Montenegro, and Slovenia have also had mass demonstrations against their governments' support of Vucic.

We can assess with moderate confidence it is highly likely demonstrations against Aleksandar Vucic will continue until the status quo changes. We can also assess with moderate confidence that it is likely that tensions between Serbia, Croatia, and other countries that are having students deported will continue to rise.

Weekly Intelligence Brief

Editor-in-Chief
Tessa Bentley

Associate Editors
Aubrey Belanger
Jordan Maple

For access to past issues and other Chanticleer Intelligence Brief projects, visit our website, cibrief.org/publications/wib

