Cyber threat activity related to the Russian invasion of Ukraine (cyber.gc.ca 2022)

Russian and Russia-linked cyber activity within Ukraine

We assess that Russian cyber operations have almost certainly sought to degrade, disrupt, destroy, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public's access to information. [3] Russian state-sponsored cyber threat actors will almost certainly continue to perform actions in support of the Russian military's strategic and tactical objectives in Ukraine.

Since the 2014 Russian annexation of Crimea, Ukraine has significantly improved its cyber security posture, including with recent assistance from European Union (EU) and Five Eyes (Australia, Canada, New Zealand, United Kingdom, and US or FVEY) governments and technology companies. [4]

Following Russia's invasion of Ukraine on February 24, 2022, likely Russian threat actors conducted several disruptive and destructive computer network attacks against Ukrainian targets, including Distributed Denial of Service (DDoS) attacks and the deployment of wiper malware against various sectors, including government, financial, and energy. Cyber operations have often coincided with conventional military operations.

To date, there are eight tracked malware families that Russia-linked cyber threat actors have used for destructive activity against Ukraine: WhisperGate/Whisperkill, FoxBlade (HermeticWiper), SonicVote (HermeticRansom), CaddyWiper, DesertBlade, Industroyer2, Lasainraw (IsaacWiper) and FiberLake (DoubleZero). [5]

In mid-April, Russian state-sponsored cyber threat actors launched four different variants of a new malware at various Ukrainian targets. Cyber security firms have attributed these attacks to a group known as Armageddon (aka Gamaredon/Shuckworm), which has been linked to Russia's Federal Security Service (FSB). [6]

Economics of Malware