WILSON MEMO

Wilson Center
Congressional Relations

Ransomware & Russia: Advancing Responsible State Behavior

The Problem

Ransomware attacks have increased in scale, scope and cost over the past five years. Four major factors are responsible:

1. As more companies and organizations have agreed to pay ransoms to recover encrypted data, ransomware attackers increased their ransom demands to millions of dollars.

2. The attack model shifted from individual targets to large organizations and managed service providers – including those securing the software supply chain, infiltrating the most trusted of networks that exist – to target more victims at once (e.g. the IT management software Kasaya).

3. Ransomware-as-a-service, in which criminal software developers lease ransomware to anyone who can pay, makes this capability available to those who want to launch ransomware attacks without technical knowledge.

4. The problem was made worse by the rapid move from office computer networks by employees to work from home during the COVID-19 pandemic, drastically increasing the vulnerabilities available to ransomware attackers (e.g. spear-phishing and unknown levels of security across personal devices and personally-configured and managed Internet).

A majority of the criminal groups providing ransomware as a service are based in Russia or surrounding countries. Three recent high-profile ransomware attacks over the last few months – including those targeting access to gas and meat – directly impacted the US economy and national security, and were launched from within Russia's borders.

The Problem

While the US has established a task force to prevent and reduce the impact of ransomware attacks, **diplomatic engagement with countries from where ransomware attacks originate will be necessary to truly stem the tide of attacks** as the economic model continues to reward.

There is a complicated history between Russia and the US on cybersecurity, including the US reportedly deploying American computer code inside Russia's electric grid and Russia's attack on the Solar Winds software security supply chain.

Where We Stand

Stopping ransomware attacks is an urgent problem with consequences for all Americans, not just big companies and tech interests. These attacks risk becoming Russia's asymmetric weapon of choice against the United States.

wilsoncenter.org
@WilsonCongress
Office of Congressional Relations

Design by Jessica Hunsinger

WILSON MEMO

Wilson Center
Congressional Relations

Ransomware & Russia: Advancing Responsible State Behavior

Where We Stand

Five American presidents have negotiated with President Putin. Their experience demonstrates that success comes from adopting a focused agenda, clear conditionality and direct, private communication — not public chest-thumping. Putin may hope to extract concessions from the United States in exchange for cooperation — for instance, acquiescence to Russia's domestic Internet censorship as a cybersecurity issue, a long-standing Russian priority. Putin may not even try to avoid future sanctions, which he probably considers an inevitable and even acceptable cost of forcing Washington to deal with Moscow as a great power.

Putin's possible reluctance to make concessions means that President Biden will have to be prepared to follow through, including by working urgently to reassure and assist European and Asian allies whose economic interests would be affected by sanctions. Trading partners in Europe and Asia — which import considerable amounts of Russian energy — could face a painful choice between winding down energy contracts impacted by sanctions and losing access to Russia as an export market, or losing access to U.S. markets and currency.

Negotiation Tactics

A bilateral technical group has been established between Russia and the US to share information, but concerns remain that these discussions might not address the root cause of ransomware attacks: identifying and stopping activity of the biggest groups operating within Russia. **The goals for negotiations with President Putin must be practical, reasonable and realistic**, and they must be backed by consequences for non-compliance in order to be taken seriously. The threat of sanctions on oil and gas companies may be an effective tool to encourage the Russian government to stop allowing these attacks to occur as they would threaten a large portion of the Russian government's revenue.

Information from Wilson Experts

Meg King & Matthew Rojansky

Director of Wilson Center Science and Technology Innovation Program (STIP). Learn more about Ms. King here.

Director of the Kennan Institute at the Wilson Center. Learn more about Mr. Rojansky here.

Go Deeper! More Resources

The Washington Post
Ransomware attacks won't stop unless Biden keeps the pressure on Putin

CTRL Forward: Wilson Center STIP
Deterring Cyber Disaster