Twitter Thread by ≡l≡v≡nth



≡l≡v≡nth
@3L3V3NTH

Kaspersky speaks on US government ban and a closed Russian internet | ZDNet

■■

https://t.co/AMPtjUBKgE

2017-

Trump signs into law U.S. government ban on Kaspersky Lab software | Reuters https://t.co/YUekOuHl7Z

May 2019-

Kaspersky Lab Joins Forces with SolarWinds to Help MSPs Deliver Automated Cybersecurity Protection to Customers https://t.co/jm1rbWxERM

Sept. -2019

U.S. Finalizes Rule Banning Kaspersky Products From Government Contracts https://t.co/RjSrtXUkeW

"Legislators enacted the law in response to concerns from the U.S. intelligence community that Kaspersky executives—some of whom are former Russian intelligence officers—have close ties to Russian government officials. U.S. officials also expressed concern that Russian law

would compel the company to share sensitive cybersecurity information on U.S. agencies gleaned through their platform with the Russian government.
The rule restricts any federal agency from purchasing or otherwise “contracting for hardware, software and services developed or

provided by Kaspersky Lab or its related entities, or using any such hardware, software or services in the development of data or deliverables first produced in the performance of the contract,” as stated in the contract clause added to the Federal Acquisition Regulation.

The rule notes this includes subcontractors at all levels."

"So what we are trying to do, working with the IT sector, the comp sector, and the rest of the federal interagency is get everybody on the same page in terms of intelligence and threat information sharing. We took a step two years ago, September 2017,
https://t.co/Ezf3CpdZFG

issuing a directive across the federal government that said, 'You know what, we've taken a look at Kaspersky anti-virus products and determined them to be too risky to be deployed within federal networks.'

And the decision, or the rationale behind it was anti-virus

operates at a pretty broad level across systems below which we usually monitor. In fact, the AV is the thing that actually does the monitoring, sweeps for data. And really effective AVs, anti-virus products, take the data, or the files, the anomalies they find, and they

send it back to a central collection point.

In the case of Kaspersky, that was Moscow. And we also know the legal system in Russia, it's not really known for meaningful judicial review, the balance and checks and balances that we have here in the US. And we know that there

are laws that compel telecommunications companies and tech companies to comply with the intelligence service.

So we kind of added this all up. And then you kind of look at the relationships between Kaspersky leadership and the Putin regime. And we said, 'All right,

theoretically, we've got a company that is delving into the depths of the US federal government that the FSB or the SVR, or GRU could operationalize."

Quote from @C_C_Krebs ^