


A Spectrum of State Ransomware Responsibility

 pylos.co/2021/09/09/a-spectrum-of-state-ransomware-responsibility/

Joe

09/09/2021



Questions concerning responsibility for the current epidemic of ransomware events are common, and seek to identify some concrete party to hold accountable for incidents. Yet the immediate perpetrators – largely (but not exclusively) criminal gangs operating in Eastern Europe and Russia – either represent too remote an entity for blame, or remain inaccessible from any consequences for their behavior. The latter point is interesting, and gives rise to theories that state entities, especially Russian authorities, overlook the operations of these groups to further their own notionally disruptive ends.

As previously discussed, ransomware operations contain at least as many, if not more, risks for state entities as benefits. Yet we should not assume all authorities employ accurate or especially deep risk calculations. Therefore, irrespective of actual benefit, we are faced with the interface between criminal entities and state authorities. That state entities are involved in ransomware operations is beyond doubt – such has been strongly suggested if not proven in cases like ColdLock, more recent Exchange exploitation, and the WannaCry event, and

reasonably considered in cases such as the LockerGoga incident at Norsk Hydro. Yet the question of state *control* or *responsibility* for such operations when conducted *by criminals* in permissive environments is more vexing.

Recent, in-depth reporting from Recorded Future implies that links between Russian criminal entities and state authorities are rather robust and derive from long-standing links between state intelligence services and criminal actors. The report is quite thorough in gathering and evaluating evidence, but conclusions bear further scrutiny. Notably, a significant tension exists between instances where members of the Russian criminal ecosystem were very directly co-opted by state entities, and looser relationships where the existence of such entities is merely permitted for one of a number of reasons. While the *effects* of such activity may be the same, the *reasons* behind such actions are drastically different, and should be taken into account when evaluating the degree of state culpability in ransomware operations.

At this time, we should familiarize ourselves with a concept long known but seldom recognized in cyber operations and intelligence analysis: the spectrum of state responsibility for cyber incidents. Originally distilled by Jason Healey and since refined or expounded on by others, the idea posits that state association with cyber events is not a binary proposition. Instead, there exist many degrees of state involvement in cyber-nexus events:

The Spectrum of State Responsibility

1. **State-prohibited.** The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated.** The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

As seen in the list above, responsibility ranges from willingness (but inability) to block or interrupt cyber events emerging from their territory to benign neglect to active encouragement to direct involvement in operations. While the above represents merely a model of activity, it remains instructive by showing analysts and others that many gradations exist defining state interaction with cyber events.

In some cases – potentially most notable with lack of action by Nigerian authorities against Business Email Compromise (BEC) entities operating in their country – states may lack the institutional ability to effectively respond (without significant external assistance) to malicious activity originating from their territory. In others, presumably criminal operations may be subsumed within or represent extensions of state-directed operations. Yet neither case appears to apply to Russian-nexus cybercrime operations. While the Russian state may have persistent issues dealing with criminality, the country remains a vaguely authoritarian society with democratic trappings – meaning if ransomware gangs were a point of particular

interest, they could (and likely would) be efficiently dealt with by authorities. At the other extreme, a state able to execute such exquisite intrusions and reasonably deniable events ranging from SUNBURST to NotPetya would appear to have little use for indiscriminate ransomware operations as a tool of state policy given other available options.

Based on the above, any assessment of Russian government culpability for ransomware operations must first determine, just what level of action (or inaction) establishes responsibility? If the measure of responsibility hinges on *negative* observations (i.e., neglect or avoidance), then we must also determine whether such actions are out of *deliberate* ignorance or more general *institutional failure*. If we posit that the Russian state is in firm control of its society, then ransomware operators functioning without sanction would appear to be a very *deliberate* choice by the Russian state. However, Russia sadly appears to be a polity afflicted by corruption, state and institutional capture, and collisions between ruling authority and popular interests. In such an environment, legal sanction for entities operating almost exclusively outside the territory of the state would appear to be either a low priority – or one of a number of opportunities for enrichment through bribes and other mechanisms.

From the above, we must ask, given the diseased institutional state of the Russian Federation, whether the entity even has the capacity to reign in ransomware operators. While collaborations between intelligence entities and criminal elements may continue to take place for various opportunistic reasons, wholesale disruption and shutdown of entities primarily impacting non-Russian entities would appear a low priority for authorities within the compromised state. Looking back to our spectrum of state responsibility, while Russian authorities appear to aspire to and occasionally reach higher levels of interaction with respect to their criminal underground, more often than not institutional failures and limitations mean such criminal activities take place irrespective of state agreement or disapproval.

Thus imaging a grand conspiracy of Russian-directed ransomware operations against EU and North American entities as a sort of covert disruptive exercise appears nonsensical. At best, Russian authorities retain weak (if any) authority over such groups, exercised only in those rare occasions when a truly critical (e.g. domestic) interest is threatened. At worst, the Russian cybercrime scene resembles a Hobbesian war of all against all, so long as effects are not significantly felt domestically, a nearly failed state can do little but watch idly while pursuing more immediate existential threats.

We may find it intellectually comforting to think that some grand conspiracy lies behind the disruptive events that impact entities ranging from hospitals to school districts to everyday commerce. Yet the totality of available evidence and understanding of circumstances overwhelmingly suggests a significant distance between Russian state authority designs and the predations of Russian-based criminal enterprises. Searching for a singular, all-encompassing “bad guy” to blame for events is a common feature of the human condition. But in the case of ransomware operations, events are too diffuse and complex to support such attribution.