RANSOMWARE
TASK FORCE

ROADMAP TO POTENTIAL PROHIBITION OF RANSOMWARE PAYMENTS

SUMMARY MEMO FROM THE RTF CO-CHAIRS | April 10, 2024

Michael Daniel
Cyber Threat Alliance

Jen Ellis
NextJenSecurity

Michael Phillips
CFC Underwriting

Megan Stifel
Institute for Security + Technology

John Davis
Palo Alto Networks

Chris Painter
former cyber diplomat

Philip Reiner
Institute for Security + Technology

Kemba Walden
Paladin Global Institute

Overview

We, the RTF Co-Chairs, have developed steps that governments and the private sector could take together to reduce the need for a prohibition on ransomware payments, or alternatively could provide a roadmap to facilitate an eventual imposition of a prohibition of ransomware payments.

We recognize that ransomware actors are inherently profit-motivated, and therefore a ban on payments could eventually result in less criminal activity. However, for several reasons detailed below, we believe a ban on payments under current circumstances will likely worsen the harms both for direct victims and, in turn, for society and the economy. In cases where bans have been introduced in limited ways (e.g., governments prohibiting themselves from paying ransoms), there has not been a clear decrease in ransomware attacks against these entities.

At present, the limited data available indicates that the majority of organizations globally are still underprepared to defend against or recover from a ransomware attack. This preparedness gap remains particularly problematic in resource-constrained critical sectors that are currently being heavily impacted by ransomware attacks, such as healthcare, education, and government. As such, a strong focus on operational engagement and aid that increases the preparedness of organizations in all sectors—most particularly those providing or supporting critical infrastructure—is essential

This document is the sole view of the Ransomware Task Force Co-Chairs, as listed above. It does not necessarily reflect views of their organizations, nor of the Ransomware Task Force as a whole.

to enable these organizations to better resist ransomware threats. Additionally, governments and the technical community need to strengthen victim support to give organizations who are affected by attacks alternative options for recovery beyond paying the ransom.

Additional downsides to a payment ban include concerns regarding its impact on reporting of ransomware incidents and the practicalities of a proliferation of exceptions. On the one hand, a no-exception ban could drive payments "underground," putting them outside the view of investigative authorities. On the other hand, if exceptions are allowed, then the pressure to add exceptions will increase over time as governments confront the realities of disrupted services. Further, if the exceptions to the ban are public knowledge, then ransomware actors will preferentially target organizations in the excepted categories. If the exception requires organizations to apply for a waiver, the number of organizations using such a system will be small, as organizations typically want to pay a ransom in order to make the problem go away as quickly and quietly as possible. Having to wait on a time-consuming application process is directly at odds with this. Determining the consequences if an entity were to violate the ban on payments is also a difficult decision, as most entities would like to remain within the law but may consider alternatives if the perceived cost of abiding by the law are too high. Additionally, criminals may test a government's resolve to enforce a ban by targeting attacks against organizations that provide services governments cannot tolerate being disrupted and that are least likely to have sufficient resilience.

We therefore believe that the most reasonable and effective approach to reducing payments, including the potential for eventually implementing a ban on payments if deemed relevant by national authorities, requires a multi-year approach based on milestones. To be clear, even if governments move aggressively to meet these milestones, it will take several years following the start of a process before prohibitions could be considered as one possible effective step.

Below are 16 proposed milestones that should be pursued to make this approach effective, falling into 4 different lines of effort. These milestones can and should be pursued concurrently. For example, many small businesses cannot tolerate a long-term disruption to their operations and they will cease to operate if they cannot bring in revenue. Therefore, governments cannot pursue one line of effort to the exclusions of the others if they want to reduce the impact of ransomware.

While some governments have made some progress against these milestones, considerable work remains even in the most proactive jurisdictions. These milestones are primarily based on recommendations made in the Ransomware Task Force report, and include reference numbers and the original proposed timelines for each Action in the RTF report. More details for each milestone can be found in the report.

Line of Effort 1: Ecosystem Preparedness

Organizations across the digital ecosystem need to be more prepared to deal with ransomware attacks. Key milestones for hardening the ecosystem include:

- **Develop a Ransomware Framework** to provide a national standard for ransomware preparation and response to create a foundation for organizational compliance. This Framework needs to be adaptable and relevant to organizations of different sizes, maturity, and risk profiles. (3.1.1) [12 - 24 months]
- **Raise awareness and understanding through national campaigns** aimed at organizational leaders, as well as operational staff. Leaders of organizations of all sizes and sectors need to understand that ransomware is relevant to their organization, and that action must be taken to protect themselves. (3.2.1, 3.2.2) [6 - 18 months]
- **Provide financial incentives** for entities to comply with the Ransomware Framework, by expanding grants, regulatory fine alleviation, or tax breaks. (3.4.2 - 3.4.5) [6 - 24 months]
- **Mandate limited baseline security measures** for critical infrastructure organizations, Managed Security Providers, and local governments, with grant funding available for those in compliance with the Ransomware Framework. (3.3.2, 3.3.3) [6 - 12 months]
- **Ensure all information-sharing pathways are robust**, including with cryptocurrency entities, incident responders, insurers, and law enforcement. (2.1.3, 2.3.1, 4.2.2 - 4.2.3) [12 - 24 months]

Line of Effort 2: Deterrence

As part of the journey towards prohibiting ransom payments, governments should lay the foundations for increased deterrence of ransomware crimes. Milestones include:

- **Issue formal statements through diplomatic channels** that governments will target ransomware criminals internationally using a range of instruments of national power. (1.1.1) [Immediate]
- **Form an international law enforcement partnership** to target ransomware criminals. (1.1.2) [3 - 6 months]
- **Establish Interagency Working Groups and Joint Ransomware Task Forces** to coordinate government disruption activities. (1.2.1, 1.2.2) [Immediate]

Line of Effort 3: Disruption

For payment bans to be credible, governments must have improved disruption capabilities in place. Milestones include:

- **Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading “desks” to comply with existing laws**, and ensure strict enforcement and swift penalties. Work with allies to implement similar approaches in their jurisdictions. (2.1.2) [12 months]
- **Engage in regular, sustained, frequent disruptive action** on ransomware criminal infrastructure, cryptocurrency seizure, and criminals themselves, in coordination with

international law enforcement. The U.S. government should lead these disruption activities with support from the private sector. (1.2.3) [3 months]

- **Leverage victim data aggregation in the global cyber insurance market** to support international law enforcement efforts and seek civil liability and recovery opportunities. (2.1.5, 2.1.7) [6 - 12 months]

Line of Effort 4: Response

Prior to any prohibitions going into effect, governments could disincentivize ransom payments by meeting the following milestones:

- **Enact ransomware emergency response authorities** and create a Ransomware Response Fund to aid recovery and disincentivize payment of a ransom. These authorities and the funding would still be needed once prohibitions go into effect, because ransomware attacks will still sometimes occur and succeed. (4.1.1 - 4.1.2) [12 - 24 months]
- **Engage with insurer consortiums to reflect prohibition and its policy predicates** in insurance and reinsurance contracts and services. These include key milestones such as the structure and function of a Ransomware Response Fund, the adoption of best practices with respect to security standards in underwriting and enterprise risk management, the satisfaction of state insurance department obligations, and the meeting of appropriate risk capital requirements. (2.1.7, 4.1.1 - 4.1.2) [12 - 24 months]
- **End tax deductibility of ransomware payments** and enhance cyber risk disclosure requirements for publicly traded companies. (not in report) [6 - 12 months]
- **Mandate reporting of ransomware incidents** to the federal government. This step would go beyond what the RTF report recommends, which was only to disclose an incident where a ransom is paid. (4.2.3 - 4.2.4) [6 - 12 months]
- **Mandate that organizations conduct due diligence and cost benefit analysis** prior to paying ransoms. (4.3.1 - 4.3.2) [12 - 24 months]

Implementing a payment prohibition

Any government that chooses to pursue a ransom payment ban should consider two additional factors beyond the milestones listed above:

1. **Method for implementation**: Although implementing a payment ban under existing statutes might be possible in some countries, such as under the International Emergency Economic Powers Act in the United States, new statutes focused on ransom payments may prove more durable and would send a stronger signal to malicious actors. Further, using legislative processes would enable governments to build greater consensus around payment prohibitions.

2. **Phasing**: Payment prohibitions can be implemented in a phased manner over time. For example, a prohibition could be enacted on public entities before it is extended to the private sector. Although current evidence does not show that payment prohibitions in the public sector have reduced ransomware attacks, such restrictions could serve other policy goals, such as not having tax dollars support criminal activity or encouraging organizations to invest more in preparedness and resilience. These other goals may outweigh the downsides to payment bans described above.