THE RANSOMWARE TASK FORCE: **ONE YEAR ON**

MAY 2022

RANSOMWARE TASK FORCE

THE RANSOMWARE TASK FORCE: ONE YEAR ON

RANSOMWARE
TASK FORCE

May 2022

Contents

Introduction

On April 29th, 2021, the **Ransomware Task Force** (RTF) published *Combating Ransomware: A Comprehensive Framework for Action* ("the Report"), which offered 48 recommendations for industry, government, and civil society action designed to deter and disrupt the ransomware business model, and to help organizations prepare for and respond at scale to such attacks. In the year since, we have seen a great deal of action to combat ransomware, yet we have also seen the numbers of observed incidents continue to rise even as stakeholders focus on the threat itself. This summary briefly discusses some of the ransomware-related activity of the last year, its impact, the current threat level, and our recommendations for moving forward, highlighting the following takeaways:

- The work that has been undertaken to combat ransomware in the past year was unprecedented and laid a strong foundation for future actions.
- The threat landscape evolved along with the financial and geopolitical forces shaping global affairs and the full scope of the ransomware threat remains unknown because of a lack of sufficient attack and payment data.
- The same coalition that assembled a year ago remains ever vigilant and active in this fight via the RTF because a unified global effort is needed to combat the evolving ransomware threat.

This is not the time for complacency; it is the time for action.

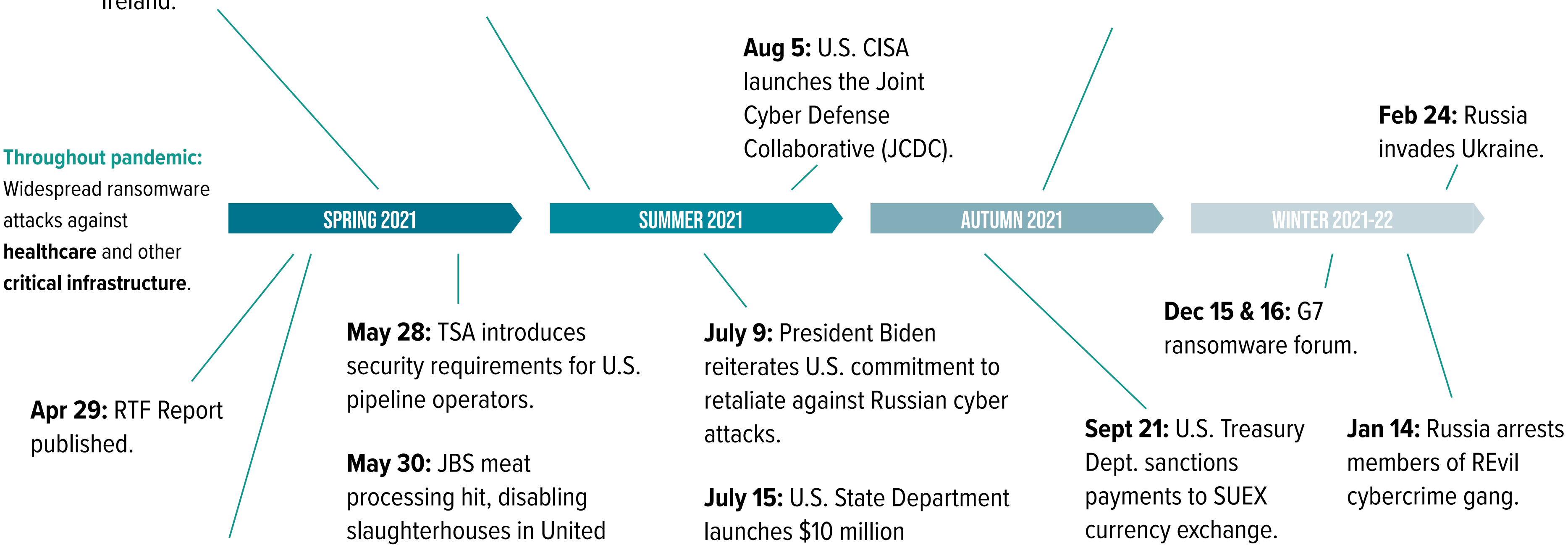
2021: An Inflection Point for Ransomware

The Institute for Security and Technology (IST), in collaboration with more than 60 public and private partners, convened the RTF in response to prolific ransomware attacks against healthcare organizations and local governments throughout the pandemic, at a time when the essential services delivered by these organizations were paramount, as they remain today. While ransomware had been a threat for some time, over recent years, it has escalated and matured into a vibrant and lucrative criminal industry. The impact of its continued rise through the pandemic led members of the RTF to believe that ransomware had become a national security threat in the United States, Canada and the United Kingdom—all of whom participated in the RTF—and in various other highly targeted countries.[1] While the ransoms quickly escalated to the millions, ransomware's fundamental threat to industry and society quickly became just as impactful. This necessitated a comprehensive response.

One week after the RTF published its report, the United States suffered its most high profile ransomware attack against its critical infrastructure when the DarkSide criminal group attacked the Colonial Pipeline Company, which delivers gasoline and jet fuel to many of the Eastern and Southern states. The attack resulted in Colonial shutting down its pipelines for six days, which created fuel shortages that disrupted road and air travel across the Southeast of the country. In response, the Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C. to keep fuel supply lines open, and the issue became major news across the United States, with President Biden addressing the nation about the attack.

A week later, a ransomware attack shut down Ireland's government agency for healthcare administration, the Health Service Executive (HSE). The attack resulted in hospitals across Ireland suspending health services. Two weeks later, a ransomware attack disrupted meat processing for JBS, the largest meat processing company (by sales) in the world, resulting in scarcity and price rises for food staples in the United States and globally. Individually, all three events would have generated considerable press and attention, but seen together across a span of three weeks, they painted a very tangible, stark picture of the threat ransomware increasingly posed to critical infrastructure, and thus to our economic health, quality of life, and safety; and at the most fundamental level, to many nations' security.

Ransomware Timeline 2021



Throughout pandemic: Widespread ransomware attacks against **healthcare** and other **critical infrastructure**.

Apr 29: RTF Report published.

May 7: Colonial Pipeline hit by DarkSide ransomware gang; pipeline temporarily shutdown.

May 14: Irish Health Service Executive hit; healthcare services suspended across Ireland.

May 28: TSA introduces security requirements for U.S. pipeline operators.

May 30: JBS meat processing hit, disabling slaughterhouses in United States, Canada, and Australia.

June 6: U.S. Justice Dept issues guidance on ransomware and digital extortion investigations and cases.

June 13: G7 commits to tackling cybercrime.

June 16: President Biden addresses attacks on U.S. critical infrastructure with President Putin.

July 9: President Biden reiterates U.S. commitment to retaliate against Russian cyber attacks.

July 15: U.S. State Department launches $10 million reward for tips connecting cybercriminals to nation states.

July 20: Second round of requirements for US pipeline operators.

Aug 5: U.S. CISA launches the Joint Cyber Defense Collaborative (JCDC).

Sept 21: U.S. Treasury Dept. sanctions payments to SUEX currency exchange.

Oct 1: OFAC sanctions named ransomware gangs.

Oct 6: U.S. Justice Dept. announces National Cryptocurrency Enforcement Team.

Oct 13 & 14: The White House hosts governments from 30 nations to launch Counter Ransomware Initiative.

Oct 21: REvil cybercrime gang temporarily forced offline by multi-country disruption campaign.

Dec 15 & 16: G7 ransomware forum.

Jan 14: Russia arrests members of REvil cybercrime gang.

Feb 24: Russia invades Ukraine.

Governmental Action to Address Ransomware

Confronted with the intensifying and critical realities of the threat, the Group of Seven (G7) governments that make up the world's wealthiest democracies met for their annual summit in June 2021,[2] mere weeks after the JBS attacks. Ransomware and cybercrime were an important topic on the agenda and the resulting Communique detailing the G7's pledges stated:

> *"We also commit to work together to urgently address the escalating shared threat from criminal ransomware networks.* ***We call on all states to urgently identify and disrupt ransomware criminal networks*** *operating from within their borders, and hold those networks accountable for their actions."*[3]

The Communique went on to call out Russia, charging its leaders to *"identify, disrupt, and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes."* President Biden underlined this emphasis on Russia's role days later when he brought the matter up directly at a summit with President Putin.[4] The U.S. President drew a line, demanding that attacks against the sixteen categories of U.S. critical infrastructure cease or the United States would take further action.

This leadership at the executive level exemplified recognition of, and response to, ransomware as a threat to national security. The commitment to stabilization was a watershed moment, setting a tone for a deep focus and hard work on this critical issue from various governments, including those of the G7. As described herein, the U.S. government led publicly with numerous measures to clarify expectations for preparation and response for critical infrastructure,[5, 6, 7, 8] create more alignment and whole-of-government focus on deterring, disrupting, and prosecuting ransomware actors,[9] while reducing opportunities for attackers to realize a payday.[10] In October, the United States also hosted a meeting with government officials from 30 nations to launch the Counter Ransomware Initiative (CRI). This meeting resulted in a joint statement and pledge for follow up actions that proved the impact of an international coalition.[11]

These government actions closely align with the RTF's recommendations. As noted in the Report, there is no silver bullet for eradicating the ransomware threat; rather doing so requires a multitude of ongoing efforts and subtle but substantial changes across the Report's four pillars to **deter**, **disrupt**, **prepare**, and **respond** to ransomware threats. Various governments—together with industry actors—have adopted this comprehensive approach, and the RTF has worked closely where possible to provide insight and feedback to refine proposals and avoid unintended consequences.

An Incomplete View

Despite substantial focus and effort from governments and other institutional leaders, supported and championed by the RTF, the full impact of these actions has not yet been seen and there is more to be done. Adoption of preparation best practices continues to be slow, particularly among small-to-medium businesses (SMBs), who may not face the greatest financial exposure alone, but collectively are incredibly important, and some of whom may be future giants of industry. Opportunities for attackers abound, and high ransoms that created headlines in the first half of 2021 continue to draw criminals to participate in the ransomware market. Business is booming, with indications of evolving tactics, techniques, and procedures (collectively, TTPs) being observed.

According to Crowdstrike, ransomware attacks increased by 82% between 2020 and 2021.[12] They reported 2,686 attacks in 2021 up from 1,474 attacks recorded in 2020. Similarly, Chainalysis reported that victims paid over $602 million in ransom payments in 2021, a 70% increase in the payments they observed in 2020.[13] Yet, while security and cryptocurrency researchers are pointing to these increases continuing in 2022, law enforcement, governments and cyber insurers are seeing reports of ransomware incidents slow down or even decrease.[14]

The lack of clarity and agreement on overall attack trends highlights one of the most significant challenges in understanding and addressing the ransomware scourge, namely the insufficiency and inconsistency of reporting. The data we have is largely cobbled together through collaborations among law enforcement, government agencies, insurers, and researchers, but even this patchwork view is incomplete. The resulting picture fails to capture the scope, scale, and impact of ransomware attacks, making it hard to accurately interpret available and incomplete data to assess the efficacy of actions being taken. This situation should improve as reporting requirements come into effect,[15] but that takes time that we do not have while the threat landscape continues to evolve.

The willingness of victims to report incidents is likely an additional factor contributing to the lack of coherence about the direction of attack trends. Security researchers and cryptocurrency analysts are monitoring attacker-side activity visible on the dark web. By contrast, law enforcement and insurers are reliant on organizations making reports, which they often prefer not to do, particularly as sanctions and other regulatory requirements increase. Many organizations fear enforcement actions, reputational impact, and other delays caused by reporting incidents. For researchers, one other element that is currently providing more visibility of attacks is the growing double extortion trend. Researchers are able to track criminal groups selling or leaking stolen data. Due to the historic lack of clear and consistent reporting, it is unclear whether increased reports of stolen data for sale on the dark web amount to more ransomware attacks, or simply more attacks that incorporate double extortion.

2022: Ransomware in a Time of Conflict

While increased attention may account for some portion of the reported rise in attacks over 2021, many ransomware experts predict that we will see overall cybercrime rates continue to rise due to the current economic and political climate. A great deal of ransomware activity has long originated from former Soviet Union nations, and the current Russia/Ukraine conflict is likely to exacerbate this trend as sanctions, withdrawal of Western businesses, and other downstream economic effects of continuing warfare force people to seek new opportunities to make a living.

Commentators on the Ukraine conflict speculate it will not be a short-term fight, and as the effects of economic deprivation and population displacements worsen over time, we are likely to see more entrants into the cybercrime market, possibly to include ransomware.

At the start of the conflict, there was speculation that Russian-affiliated cybercrime gangs would join the war effort on behalf of the Russian state, and move away from simply financially-driven ransomware attacks. While some groups did declare support for either Russia, Belarus, or Ukraine, we have seen no significant indications of a shift away from ransomware activity and its accompanying business model. A notable development has been Contileaks,[16] a huge cache of information leaked describing the inner workings of the team behind the prolific Conti ransomware, which was used in the HSE attack.[17] The leak was reportedly the result of infighting in the cybercriminal gang after some members of the gang declared support for Russia shortly after the invasion, resulting in another member, siding with Ukraine, leaking the data in a show of retaliation and defiance. That cache provided a great deal of insight into the inner workings of just one organized criminal gang. However, despite a brief period of uncertainty, indicators are clear that Conti is once again very active.

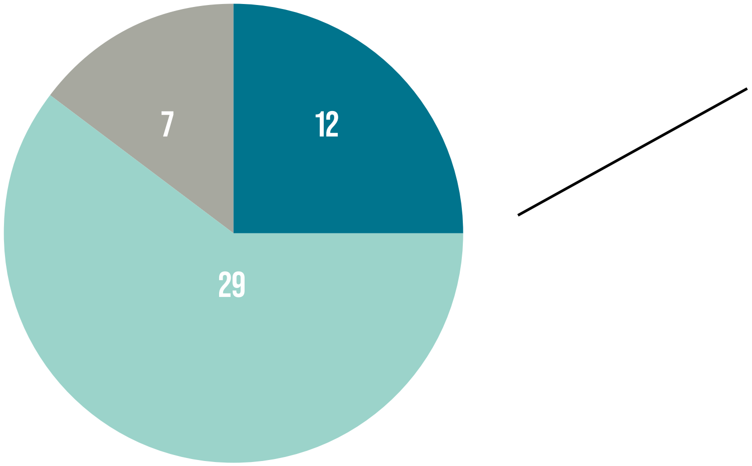
Another area where we have seen politics play a role in evolving the ransomware landscape is in its use as political activism. We have seen this phenomenon emerge this year in Costa Rica and Peru and as yet, it is unclear whether the trend will continue, and if so, how it will evolve.[18] As this activity is not primarily motivated by profit in the way that traditional ransomware attacks are, it may need different responses, likely viewed as part of a broader response to political activism.

Status of the Ransomware Task Force's Recommendations

In the following paragraphs we summarize both considerable progress as well as continuing challenges to the implementation of the RTF's recommended actions. This summary is not exhaustive. The complete assessment is available on IST's website, and will be updated over time.

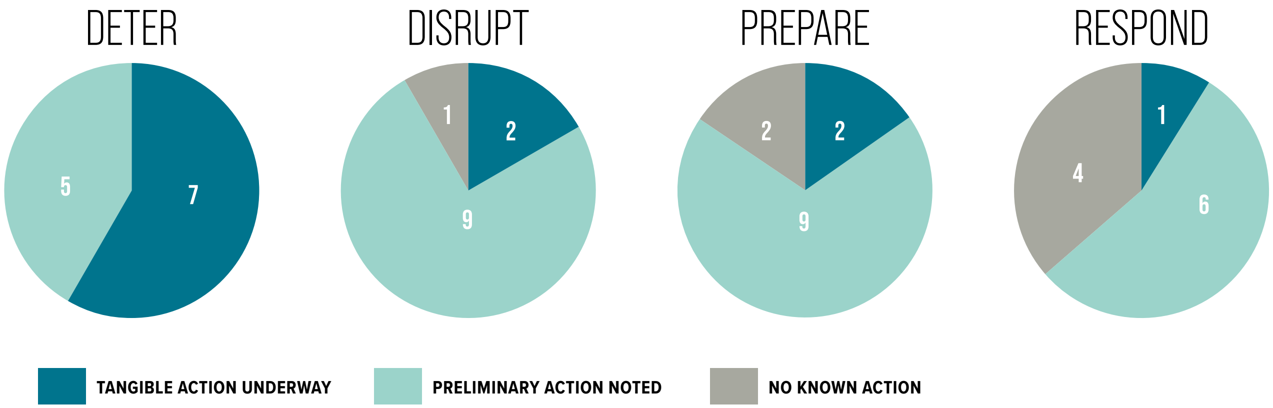
RECOMMENDATIONS SUMMARIZED

Action Underway	**12**
Preliminary Action	**29**
No Known Action	**7**

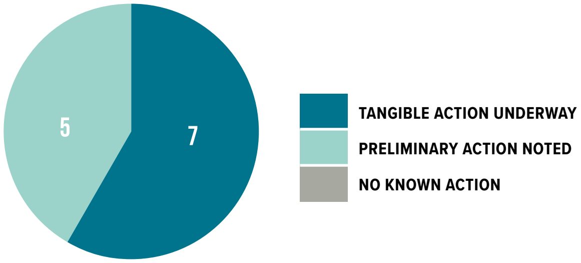


Of the 48 specific recommendations made by the Ransomware Task Force in April 2021, 12 have seen tangible progress in the year since. Preliminary actions have been observed on 29 more, while 7 recommendations have had no known action at all.

OBJECTIVES BY SPECIFIC GOALS:



Goal 1: Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy


DETER RECOMMENDATIONS, 2021–22

Over the years governments and industry have grown to recognize the cross-sector nature that cybersecurity risks present. They have evolved authorities, programs, and capabilities that help better secure critical sectors, and built key relationships both domestically and abroad to facilitate enhanced communication and coordination in addressing these risks. The RTF lauded and continues to support these developments, but also pointed out that their deployment has at times been uncoordinated, disjointed, and siloed. The RTF urges the United States and other governments to narrow these policy and operational gaps and signal internationally that ransomware remains a top enforcement priority.

Both the United States and other governments' public rhetoric shifted in 2021. In March, the U.S. Department of Homeland Security launched a Ransomware Sprint.[19] In early April, the U.S. Department of Justice launched the Ransomware and Digital Extortion Task Force.[20] In doing so, it noted that ransomware and digital extortion pose a national and economic security threat to the United States. The attack on Colonial Pipeline quickly elevated ransomware and cybersecurity to an unprecedented national priority. As noted above, President Biden addressed the issue personally, and reiterated the imperative for responsible countries to take decisive action against ransomware networks operating from within their borders. Additionally, as noted above, in June, the G7 committed to work together urgently to address the escalating shared threat from criminal ransomware networks, and in the fall of 2021, as noted above, the United States launched the international Counter Ransomware Initiative, which focuses on enhancing resilience, countering illicit finance, disruption and other law enforcement efforts, and diplomacy. Several key arrests and related actions in November 2021 exemplified that in combining capabilities, governments could be very effective at dismantling these actors.[21]

Progress has been made in key areas, with examples as follows:

- **Actions 1.1.1,** to issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority, and **1.1.2,** to establish an international coalition to combat ransomware criminals, **1.1.4,** and to convey the international priority of collective action on ransomware via sustained communications by national leaders, and **1.3.1,** to exert pressure on nations that are complicit or refuse to take action. The June 2021 summit between President Biden and Russian President Vladimir Putin, focused in part on the threat of ransomware.[22] At the 2021 NATO Brussels Summit, members acknowledged the complex, destructive, and coercive nature of attacks and their increasing frequency, and cited ransomware as an example. They endorsed NATO's Comprehensive Cyber Defense Policy to face the evolving challenge of attacks "targeting critical infrastructure and democratic institutions, which might have systemic effects and cause significant harm."[23] In October 2021, as previously noted, the White House facilitated an international meeting focused on countering ransomware. The event concluded with an unprecedented joint statement from the represented countries affirming their dedication to stem the spread of ransomware. In December 2021, the G7 gathered for an Extraordinary Senior Officials' forum on Ransomware in which senior leaders discussed ransomware threats, policy approaches, cryptocurrencies, resilience and communication, among other topics.[24] In January 2022, Russian law enforcement arrested several members of the REvil ransomware gang,[25] but on February 24, 2022, Russia invaded Ukraine, undermining any chance of continued cooperation. A few weeks prior to the invasion, U.S., U.K., and Australian cybersecurity authorities issued a joint report that provided important insight into ransomware trends globally.[26]

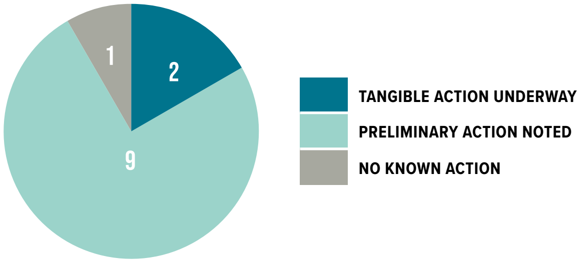
- **Action 1.2.1**, to establish an Interagency Working Group for ransomware. In June 2021, President Biden established an interagency task force focused on ransomware to coordinate and align law enforcement and prosecutorial initiatives within the U.S. government.[27]
- **Action 1.2.2,** to establish an operationally focused U.S. government Joint Ransomware Task Force to collaborate with a private-sector. In March 2022, the U.S. Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 which established a Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and to identify opportunities for international cooperation and establish mechanisms for working closely with the private sector.[28]
- **Action 1.2.4,** to make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public. In June 2021, the U.S. Department of Justice stated it would elevate investigation of ransomware attacks to a similar priority as terrorism.[29, 30] Further, as noted above, in September 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory on potential sanctions against entities that make or facilitate ransomware payments, providing some important clarification to its previous statements.[31]
- **Action 1.2.5,** to raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat. In an important step forward, the 2022 Office of the Director of National Intelligence Annual Threat Assessment highlighted ransomware and cybercrime as an important international national security issue.[32]

Though there has been important and significant progress with regard to the recommendations made in last year's RTF Report, complex challenges remain in implementing the recommendations related to deterrence. The primary challenge has been incentivizing global cooperation and action, particularly with Russia. While Russia did arrest a handful of ransomware actors and seize their related financial assets, it has done so in such a way that indicates a belief that the potential repercussions for broader inaction are easily sustained. For the most part, Russia remains undeterred from providing the safe haven identified as a core problem in the RTF report.

Deterrence has also proven challenging in resource-constrained countries. Those countries with the resources to fight ransomware's spread remain primarily focused on domestic threats. While domestic implementation and protection have been significant and are critically important, counter-ransomware efforts are more successful when international cooperation and proactive action are incentivized. As the international community takes increasingly coordinated and proactive approaches together, the global deterrence of ransomware will be more effective.

Goal 2: Disrupt the ransomware business model and decrease criminal profits

DISRUPT RECOMMENDATIONS, 2021–22



Ransomware is overwhelmingly a financially motivated crime, and as long as the profits outweigh their associated risks, attacks will continue worldwide. To effectively disrupt the ransomware threat, government agencies and industry partners must work collaboratively to reduce the profitability of this criminal enterprise and increase the complexity and risk for ransomware actors. The RTF report highlighted several important steps to enable this, including to:

1. Disrupt payment systems to make ransomware attacks less profitable;
2. Disrupt the infrastructure used to facilitate attacks; and
3. Disrupt ransomware actors themselves, through criminal prosecution and other tactics.

Today, ransom payments are generally made through the use of cryptocurrencies, making attribution of payments difficult and thereby contributing to laundering. Governments face challenges in identifying and disrupting malicious transactions while enabling cryptocurrency to still provide other positive benefits to financial systems. Government authorities' have tried to address this issue by regulating cryptocurrencies or applying sanctions to specific exchanges.

Progress has been made in key areas, including:

- **Action 2.1.2,** to require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws. In addition to the U.S. Department of Justice's establishment of the National Cryptocurrency Enforcement Team (NCET), which included a focus on mitigating the illicit use of cryptocurrency,[33] in June 2021, the Financial Crimes Enforcement Network (FinCEN) issued the first government-wide priorities and standards to prevent money laundering and countering the finance of terrorism policy.[34] Further, in September 2021, OFAC designated SUEX,[35] a cryptocurrency exchange, for allegeding facilitating financial transactions for ransomware actors and in November 2021, it announced additional sanctions against Chatex,[36] a virtual currency exchange, and its associated support network, for facilitating financial transactions for ransomware groups. In April 2022 OFAC sanctioned the largest darknet market, Hydra, as well as the ransomware-enabling virtual currency exchange Garantax, as part of a coordinated international effort to disrupt illegal offerings on the site.[37] And, in May 2022, OFAC announced its first ever sanctions against a virtual currency mixer, Blender.io, which was used by the DPRK to support malicious cyber attacks and launder stolen funds.[38] Also in May, the Treasury Department issued the National Strategy for Combating Terrorist and Other Illicit Financing. The report identifies ransomware as an ongoing international coordination priority.[39]

- **Action 2.1.3,** to incentivize voluntary information sharing between cryptocurrency entities and law enforcement. A key focus of the October 2021 international Counter Ransomware Initiative Meeting was increasing collaboration among law enforcement, intelligence and agencies, and foreign partners in order to disrupt the ransomware ecosystem.[40]

- **Action 2.1.4,** to centralize expertise in cryptocurrency seizure, and scale criminal seizure processes. In addition to creating the NCET, the U.S. Department of Justice launched a new Civil Cyber-Fraud Initiative that combines the expertise in civil fraud enforcement, government procurement, and cybersecurity.[41] The RTF has also established a cryptocurrency working group.

- **Action 2.1.6,** to launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs. In July 2021, the U.S. Department of State offered up to $10 million as a reward for information leading to the identification or location of criminal actors participating in malicious cyber activities against U.S. critical infrastructure.[42] In November 2021, it also offered up to $10 million as a reward for information related to the identification and location of individuals who hold leadership positions in the DarkSide or Sodinokibi (REvil) ransomware gangs and a $5 million reward for information leading to the arrest or conviction of individuals conspiring to participate in a DarkSide or Sodinokibi (REvil) ransomware incident.[43, 44] In May 2022, the State Department offered up to $10 million as a reward for information leading to the identification and location of individuals that hold leadership positions in the Conti ransomware gang.[45] As part of this offering, it additionally offered up to $5 million as a reward for information leading to the arrest or conviction of any individual in any country conspiring to participate in a Conti ransomware attack. The State Department linked this offer to the April 2022 ransomware attack which severely impacted the customs and taxes platforms of the Government of Costa Rica. Further, the aforementioned Civil Cyber-Fraud Initiative will play an important role in fulfilling this recommendation.

- **Action 2.1.7**, to establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management. In June of 2021, leading cyber insurers from across the country announced the creation of CyberAcuView,[46] a company dedicated to enhancing cyber risk mitigation in the cyber insurance industry. Further, the RTF has created a cyber insurance roundtable to develop solutions to address the issues raised in the RTF report.

- **Action 2.3.1**, to increase government sharing of ransomware intelligence. In March 2022, as noted above, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022. This new law establishes a Joint Ransomware Task Force composed of participants from Federal agencies to coordinate an ongoing national campaign against ransomware attacks and identify and pursue opportunities for international cooperation. The law also requires any Federal agency that receives a report of a cyber incident, including a ransomware attack, from an entity shall provide the report to the Cybersecurity and Infrastructure Security Agency (CISA) as soon as possible, but not later than 24 hours after receiving the report. Moreover, the law requires the CISA Director to share and coordinate each report.

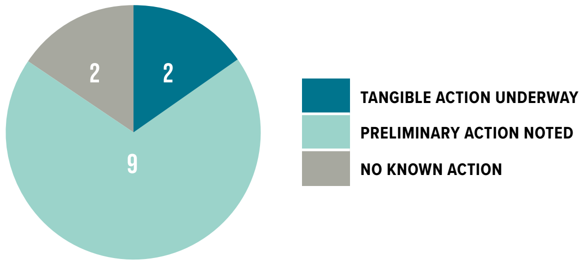
- **Action 2.3.3,** to apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure. Throughout 2021, the Department of Justice and the Federal Bureau of Investigation have taken important previously-mentioned steps to target the REvil ransomware group and others. These actions include indictments, arrests, and the seizure of funds.

Despite important progress in disrupting the actions of ransomware actors, challenges remain in implementing the RTF's recommendations. Ransomware actors deftly take advantage of legal and bureaucratic constraints in the United States and elsewhere around the globe—and largely continue to act with impunity from safe havens. As a result, there are challenges in the level of action that can be taken to disrupt. Should it be via law enforcement action, with an emphasis on arrest and prosecution? Or more of a national security action, aimed at infrastructure and the payments process against targets outside cooperative jurisdictions?

Challenges also result from the limited operational collaboration and scale of information- sharing among and between government agencies and private industry partners, thus inhibiting cooperation on disruptive actions against criminals. Ambiguity over the scope of lawful defensive measures that private-sector actors can take when countering ransomware also remains a limitation to effective response. Information provided to required and voluntary incident sharing can improve public-private collaboration to disrupt these actors, however as noted elsewhere, the pace of this reporting is also a limiting factor in nearer term impact.

Goal 3: Help organizations prepare for ransomware attacks

PREPARE RECOMMENDATIONS, 2021–22



Driving greater adoption of preparation best practices at scale continues to be a primary goal for governments, particularly among their most vulnerable or essential segments, including critical infrastructure providers and SMBs. Part of the challenge is providing detailed, actionable guidance tailored to different organizations' needs and context, without overwhelming organizations with confusing and overly complex information. At the same time, education on this topic must move beyond the echo chamber of cybersecurity to reach organizations that are not currently engaged, due to a lack of awareness or understanding of the relevance to, and potential impact on, their organization.

SMBs pursuing the adoption of best practices face difficulties due to their resource constraints and limited technical maturity. In line with the recommendations of the Task Force, many governments are instead examining the role of Managed Service Providers (MSPs) that provide technology infrastructure and services for SMBs. Proposals to update the Network and Information Systems Directive in both the European Union and the United Kingdom include greater focus on the role of digital service providers in serving SMBs and essential services organizations.[47][48] Similarly, the Center for Internet Security (CIS) is partnering with the RTF to develop a set of critical controls specifically to assist SMBs in preparing for attacks, likely including guidance for MSPs. They expect to publish these recommendations, known as the Blueprint for Ransomware Defense, during the summer of 2022.

Hand-in-hand with the need to build more understanding of the ransomware threat and related preparatory measures is the need to provide appropriate resources that support action. The RTF recommendations included measures to fund critical infrastructure and local government organizations so they can then make appropriate cybersecurity investments. Government organizations such as CISA in the United States and NCSC in the UK are also providing access to free security services and capabilities for critical infrastructure and government organizations.

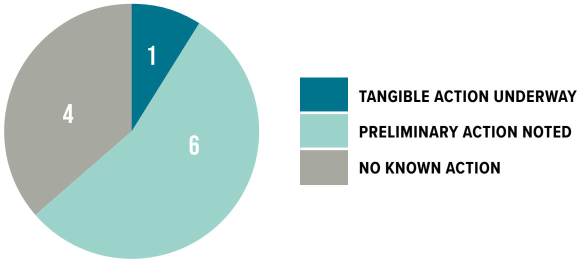
Despite the challenges, progress is being made, for example:

- **Action 3.2.2**, to run nationwide, government-backed awareness campaigns and tabletop exercises. In 2022, the scenario for Cyber Storm, DHS's cyber-related multi-day exercise, involved both operational (e.g., industrial control systems) and traditional enterprise systems, with organizations experiencing various impacts such as ransomware and data exfiltration.[49] In addition, several governments have partnered on awareness campaigns in the run up to, and throughout, the ongoing Russia/Ukraine conflict.[50] While the guidance has not specifically addressed ransomware, it is relevant, and the focus on the conflict may help draw more attention from a broader audience.
- **Action 3.3.1,** to update cyber-hygiene regulations and standards. In February 2022, the National Institute of Standards and Technology (NIST) released a profile for the Cybersecurity Framework that specifically addresses ransomware risk management.[51] It includes information for preventing, responding to, and recovering from ransomware events. In addition, this summer the Blueprint working group intends to publish the aforementioned guidance.
- **Action 3.3.2,** to require local governments to adopt limited baseline security measures. Federal legislation[52] is supporting the local government's efforts to adopt baseline security standards. Further, in November 2021, the Bipartisan Infrastructure Bill included an additional $1 billion to assist state, local, tribal, and territorial governments in deterring attacks from malicious cyber actors and modernizing systems to protect sensitive data, information, and public critical infrastructure. It also provides $100 million to help victims of a serious attack recover quickly.[53]

This progress is a solid start. We are pleased to see the level of focus on this challenge among the governments that have participated in, or worked directly with, the RTF, such as the United States, United Kingdom, and Canada. We hope that other governments around the world are taking similar action to protect their SMBs and critical infrastructure providers. It is important to recognize that driving adoption of cybersecurity best practices will always be a battle as resources are constrained and face competing demands across the business. Governments will need to continue to invest in a combination of incentives, funds, free services, regulation, and education.

Goal 4: Respond to ransomware attacks more effectively

RESPOND RECOMMENDATIONS, 2021–22



No matter how effective we become at deterring, disrupting, and preventing ransomware attacks, some percentage of attacks will succeed nonetheless. The RTF's fourth goal focused on improving the ability of individuals, organizations, and society to respond to successful ransomware attacks. Our recommendations were aimed at increasing the availability of information about ransomware attacks in terms of frequency, volume, and other characteristics; creating incentives for organizations to avoid paying ransoms; and increasing support for companies that have fallen victim to a ransomware attack.

With respect to the Task Force's key recommendations supporting this goal, the United States has made significant progress via the executive and legislative branches over the past year implementing many of our recommendations. For example, as noted above, Congress created the Cyber Response and Recovery Fund in the Infrastructure Investment and Jobs Act in November 2021 and provided $20 million per year for the next five years for the fund.[54] The U.S. Department of the Treasury has updated its guidance around ransomware payments, although additional guidance is needed.[55] As noted above, in March 2022, Congress also passed mandatory incident reporting requirements for critical infrastructure, including an additional requirement to report ransom payments after the fact, partially implementing the RTF's recommendations.[56]

Significant progress has also been made on a number of our other recommendations. For example:

- **Action 4.1.1**, to create Ransomware Emergency Response Authorities. The Infrastructure Investment and Jobs Act included emergency response authorities for the Secretary of Homeland Security.
- **Action 4.1.2**, to create a Ransomware Response Fund. Congress created the Cyber Response and Recovery fund[57] in the Infrastructure Investment and Jobs Act in November 2021, providing $20 million per year over the next five years for a total of $100 million.
- **Action 4.1.3**, to increase government resources available to help the private sector. Cybersecurity has increased as a priority across most Federal departments and agencies and almost all sector-specific agencies have expanded their programs that work with their respective sectors. For example, in February 2022, CISA released a free catalog of cybersecurity resources.[58]

- **Action 4.1.4**, to clarify United States Treasury guidance regarding ransomware payments. The September 2021 OFAC Advisory[59] begins to accomplish this, but requires more guidance because many companies remain uncertain about when it is and is not legal to pay a ransom.

- **Action 4.2.4**, to require organizations and incident response entities to share ransomware payment information with a national government prior to payment. CISA guidance and the September 2021 OFAC Advisory both suggest sharing payment information.[60][61] Additionally, the Cyber Incident Reporting and Critical Infrastructure Act set in motion reporting requirements for critical infrastructure, to include information about ransomware payments. It also encourages voluntary reporting.[62]

While significant progress has been made over the past year, federal and state governments still need to do more to support the private sector. In particular, the lack of comprehensive information about ransomware attacks continues to impede effective policy development and action against ransomware actors. Even the statistics cited at the beginning of this update reflect this problem; at best, they are estimates from a particular company's or government agency's point of view. While aggregating these different reports can provide a general sense of the trends, policy decisions and priorities should be based on more reliable data. Unfortunately, efforts to improve information sharing about ransomware attacks have been slow, due to competing priorities, legal and regulatory restrictions, and other perceived downsides.

In addition, under recently passed legislation, CISA has two years to implement the reporting requirement using the standard Federal rule-making process. While beneficial in many ways, this formal process will take considerable time, and thus an opportunity cost. The legislation only applies to entities in critical infrastructure sectors; and no general agreement exists on whether and how to extend these reporting requirements to other organizations in the ecosystem.[63] Nevertheless, the RTF will continue its efforts to implement the Ransomware Incident Reporting Network to increase the depth, breadth, and accuracy of information about ransomware attacks across the digital ecosystem.

Furthermore, many in the private sector remain confused about when it is and is not legal for them to pay ransoms. The incentive structure around ransom payments has not been adjusted significantly enough to dissuade some companies from paying ransoms.

Moving Forward to Tackle the Threat

The degree of focus and action on the ransomware threat from various governments is welcome, warranted, and necessary. It is also heartening. In particular, the level of collaboration between governments alongside coordination and leadership from the private and nonprofit sectors gives us hope for a brighter future. When the RTF published its Report, it was clear there was no silver bullet that would “solve” the ransomware problem, and that even with an “all tools of national power” approach, it would take years to fracture the ransomware business model.

The agility and dynamism of ransomware actors cannot be overstated. Since the recommendations in the Report will take time to implement and create impact, it is critical that the disruptive actions, response times, and preventive actions move as dynamically as the actors, if not more so.

Additionally, in preparing the Report, the RTF debated options for banning ransom payments, but did not make an initial recommendation. This has continued to present a challenge for policymakers. Many governments have internal policies of nonpayment of ransoms for any government entities hit by ransomware attacks. Many would like to broaden the prohibition with a view to eventually discouraging attackers from pursuing a payday through ransomware attacks. The challenge is that before attackers give up on this revenue stream, they will likely try to target organizations that are most unable to tolerate disruption, for example SMBs and critical infrastructure providers, and force them into making under-the-table payments. In recognition of this challenge, policymakers are not rushing to a prohibition, but rather have looked for paths to reduce the risk and create a more level playing field for these highly vulnerable organizations. The Report included some recommendations for achieving this path, such as offering a financial safety net to give qualifying organizations the resources to recover from attacks. These suggestions have been discussed, but at present, it appears most governments are more focused on tackling other aspects to deter and disrupt attacks, and to help organizations prepare and respond.

As stated previously, there is more work to be done, but with continued prioritization and resources, we believe **additional progress can and will be made to manage not just the ransomware threat, but also to improve the digital ecosystem for the future**. While the debated rise in observed incidents paints a gloomy picture at present, we believe the increased level of action, awareness, and visibility is positive and that with continued focus, will eventually lead to a greater level of understanding of this threat, along with an improved ability to deter, disrupt, prepare for, and respond to attacks.

Endnotes

[1] Blackfog, “The State of Ransomware in 2022,” April 4th, 2022. https://www.blackfog.com/the-state-of-ransomware-in-2022/

[2] G7 UK 2021, Carbis Bay, Cornwall, June 11-13, 2021. https://www.g7uk.org/

[3] Carbis Bay G7 Summit Communiqué, “Our Shared Agenda for Global Action to Build Back Better,” G7 UK 2021, June 13, 2021. https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-3.pdf

[4] Soldatkin, Vladimir and Pamuk, Humeyra, “Biden tells Putin certain cyberattacks should be ‘off-limits’,” Reuters, June 16, 2021. https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/

[5] Geiger, Harley, “How Ransomware Is Changing US Federal Policy,” Rapid 7 Blog, March 17th, 2022. https://www.rapid7.com/blog/post/2022/01/26/how-ransomware-is-changing-us-federal-policy/

[6] Neuberger, Anne to Corporate Executives and Business Leaders, “What We Urge You To Do To Protect Against The Threat of Ransomware,” The White House, June 2, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf

[7] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, “Colonial Pipeline Cyber Incident.” https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[8] Biden, Joseph R., Executive Order on Improving the Nation’s Cybersecurity, The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[9] Monaco, Lisa, Memorandum for All Federal Prosecutors, “Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion,” U.S Department of Justice, June 3, 2021. https://www.justice.gov/opa/press-release/file/1402001/download

[10] U.S. Department of the Treasury, Office of Foreign Assets Control, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[11] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting, The White House, October 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[12] Crowdstrike, “2022 Global Threat Report,” 2022. https://www.crowdstrike.com/global-threat-report/

[13] https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

[14] Chainanalysis Team, “As Ransomware Payments Continue to Grow, So Too Does Ransomware’s Role in Geopolitical Conflict,” Chainanalysis, February 10, 2022. https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/

[15] For example, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, (H.R.2471, Public Law No: 117-103. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471/text), and recently passed state legislation, (Associated Press, “Maryland Governor Signs Bill to Strengthen Cybersecurity,” May 12, 2022. https://www.securityweek.com/maryland-governor-signs-bills-strengthen-cybersecurity).

[16] Burgess, Matt, “The Workday Life of the World’s Most Dangerous Ransomware Gang,” Wired, March 16, 2022. https://www.wired.com/story/conti-leaks-ransomware-work-life/

[17] HHS Cyber Security Program, “Lessons Learned from the HSE Cyber Attack,” U.S. Department of Health & Human Services, Office for Information Security, February 3, 2022. https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf

[18] Marks, Joseph, “Costa Rica shows the damage ransomware can do to a country,” The Washington Post, May 10, 2022. https://www.washingtonpost.com/politics/2022/05/10/costa-rica-shows-damage-ransomware-can-do-country/

[19] U.S. Department of Homeland Security, “Factsheet: Ransomware Sprint,” April—May 2021. https://www.dhs.gov/sites/default/files/publications/21_0624_ransomware-fact-sheet.pdf

[20] Fung, Brian, “Justice Department is launching a ransomware task force,” CNN, April 21, 2021. https://www.cnn.com/2021/04/21/tech/ransomware-doj-task-force/index.html

[21] Newman, Lily Hay, “The Biggest Ransomware Bust Yet Might Actually Make an Impact,” Wired, November 8, 2021. https://www.wired.com/story/ransomware-revil-arrest-kaseya/

22 Soldatkin, Vladimir and Holland, Steve, “Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control,” Reuters, June 16th, 2021. https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/

23 North Atlantic Treaty Organization, “Brussels Summit Communiqué,” June 14, 2021. https://www.nato.int/cps/en/natohq/news_185000.htm

24 U.K. Home Office, “Chair’s summary from the G7 Interior and Security Senior Officials’ Extraordinary Forum on Ransomware on 15 and 16 December 2021,” United Kingdom Home Office, December 24, 2021. https://www.gov.uk/government/publications/g7-interior-and-security-senior-officials-meeting-on-ransomware/chairs-summary-from-the-g7-interior-and-security-senior-officials-extraordinary-forum-on-ransomware-on-15-and-16-december-2021

25 Nechepurenko, Ivan, “Russia Says It Shut Down Notorious Hacker Group at U.S. Request,” The New York Times, January 14, 2022. https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html

26 U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Alert (AA22-040A), “2021 Trends Show Increased Globalized Threat of Ransomware,” February 10, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

27 The White House, “FACT SHEET; Ongoing Public U.S. Efforts to Counter Ransomware,” October 13, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

28 Consolidated Appropriations Act, 2022, H.R.2471.117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471/text

29 Bing, Christopher, “U.S. to give ransomware hacks similar priority as terrorism,” Reuters, June 3, 2021. https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

30 Fung, Brian, “Justice Department is launching a ransomware task force,” CNN, April 21, 2021. https://www.cnn.com/2021/04/21/tech/ransomware-doj-task-force/index.html

31 U.S. Department of the Treasury’s Office of Foreign Assets Control, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

32 U.S. Office of the Director of National Intelligence, “Annual Threat Assessment of the U.S. Intelligence Community,” February 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

33 U.S. Department of Justice, Office of Public Affairs, “Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team,” October 6, 2021. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team

34 U.S. Department of Justice, Financial Crimes Enforcement Network, “FinCEN Issues First National CML/CFT Priorities and Accompanying Statements,” June 30, 2021. https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements

35 U.S. Department of the Treasury, “Treasury Takes Robust Actions to Counter Ransomware,” May 16, 2022. https://home.treasury.gov/news/press-releases/jy0364

36 U.S. Department of the Treasury, “Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange,” November 8, 2021. https://home.treasury.gov/news/press-releases/jy0471

37 U.S. Department of the Treasury, “Treasury Sanctions Russia-Based Hydra, World’s Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex,” April 5, 2022. https://home.treasury.gov/news/press-releases/jy0701

38 U.S. Department of the Treasury, “U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Target DPRK Cyber Threats,” May 6, 2022. https://home.treasury.gov/news/press-releases/jy0768#:~:text=%E2%80%9CToday%2C%20for%20the%20first%20time,to%20U.S.%20national%20security%20interests

39 U.S. Department of the Treasury, “National Strategy for Combating Terrorist and Other Illicit Financing,” May 2022 . https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf

40 Marañon, Alvaro and Pell, Stephanie, “Countering the Ransomware Threat: A Whole-of-Government Effort,” Lawfare, November 22, 2021. https://www.lawfareblog.com/countering-ransomware-threat-whole-government-effort

41 U.S. Department of Justice, Office of Public Affairs, “Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative,” October 6, 2021. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

42 U.S. Department of State, Office of the Spokesperson, “Rewards for Justice—Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure,” July 15, 2021. https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/

43 U.S. Department of State, Office of the Spokesperson, “Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice,” November 4, 2021. https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/

44 U.S. Department of State, Office of the Spokesperson, “Reward Offers for Information to Bring Sodinokibi (REvil) Ransomware Variant Co-Conspirators to Justice,” November 8, 2021. https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/

45 U.S. Department of State, Office of the Spokesperson, “Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice,” May 8, 2022. https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/

46 CyberAcuView, “Consortium of Leading Cyber Insurers Announce the Launch of CyberAcuView,” June 17, 2021. https://cyberacuview.com/press-release-june-2021/

47 European Commission, “Commission welcomes political agreement on new rules on cybersecurity of network and information systems,” May 13, 2022. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

48 U.K. Home Office, “Call for views on cybersecurity in supply chains and managed service providers,” November 15, 2021. https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security/call-for-views-on-cyber-security-in-supply-chains-and-managed-service-providers

49 U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “CISA Hosts Eighth Cyber Storm Exercise With More Than 200 Organizations,” March 14, 2022. https://www.cisa.gov/news/2022/03/14/cisa-hosts-eighth-cyber-storm-exercise-more-200-organizations

50 U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “CISA, FBI, NSA, and International Partners Issue Advisory on Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors,” April 20, 2022. https://www.cisa.gov/news/2022/04/20/cisa-fbi-nsa-and-international-partners-issue-advisory-demonstrated-threats-and

51 European Commission, “Commission welcomes political agreement on new rules on cybersecurity of network and information systems,” May 13, 2022. https://csrc.nist.gov/publications/detail/nistir/8374/final

52 National Defense Authorization Act for Fiscal Year 2022, H.R.4350.117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/4350

53 U.S. Senate Committee on Homeland Security & Governmental Affairs, “Peters Provisions to Strengthen Cybersecurity Signed Into Law as Part of Bipartisan Infrastructure Bill,” November 15, 2021. https://www.hsgac.senate.gov/media/majority-media/peters-provisions-to-strengthen-cybersecurity-signed-into-law-as-part-of-bipartisan-infrastructure-bill

54 Infrastructure Investment and Jobs Act, 2021, H.R.3684, Public Law No: 117-59. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/3684/text

55 U.S. Department of the Treasury, Office of Foreign Assets Control, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

56 Consolidated Appropriations Act, 2022, H.R.2471, Public Law No: 117-103. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471/text

57 Infrastructure Investment and Jobs Act, 2021, H.R.3684, Public Law No: 117-59. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/3684/text

58 U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “CISA Launches New Catalog of Free Public and Private Sector Cybersecurity Services,” February 18, 2022. https://www.cisa.gov/news/2022/02/18/cisa-launches-new-catalog-free-public-and-private-sector-cybersecurity-services

59 U.S. Department of the Treasury, Office of Foreign Assets Control, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

60 U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “Ransomware Guide,” Stop Ransomware, February 18, 2022. https://www.cisa.gov/stopransomware/ransomware-guide

61 U.S. Department of the Treasury, Office of Foreign Assets Control, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

62 Consolidated Appropriations Act, 2022, H.R.2471, Public Law No: 117-103. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471/text

63 Consolidated Appropriations Act, 2022, H.R.2471, Public Law No: 117-103. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471/text

Appendix:

Status of RTF Recommendations by Specific Objective

GOAL 1: DETER RANSOMWARE ATTACKS

Objective	Rec.	Description	Lead	Timeline
Signal that ransomware is an international diplomatic and enforcement priority	🟩 1.1.1	**Issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority.**	National governments	Begin groundwork immediately; declarations to be issued upon international group meeting
	🟩 1.1.2	**Establish an international coalition to combat ransomware criminals.**	U.S. lead, in coordination with international partners	3-6 months
	🟩 1.1.3	**Create a global network of ransomware investigation hubs.**	U.S. lead, in coordination with international partners	9-12 months
	🟦 1.1.4	**Convey the international priority of collective action on ransomware via sustained communications by national leaders.**	White House	Begin groundwork immediately; declarations ongoing
Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House	🟦 1.2.1	**Establish an Interagency Working Group for ransomware.**	White House / NSC	Immediate
	🟦 1.2.2	**Establish an operationally focused U.S. government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub.**	White House in coordiation with private industry	Immediate
	🟩 1.2.3	**Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign.**	White House in coordiation with private industry	3-6 months
	🟦 1.2.4	**Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public.**	DOJ and congress, in coordination with international equivalents	9-12 months
	🟩 1.2.5	**Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat.**	White House (via DNI)	3 months
	🟩 1.2.6	**Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns.**	White House (via DNI), coordinate with Five Eyes partners	3 months
Substantially reduce safe havens where ransomware actors currently operate with impunity	🟦 1.3.1	**Exert pressure on nations that are complicit or refuse to take action.**	DOJ and DOS	3 months, ongoing
	🟩 1.3.2	**Incentivize cooperation and proactive action in resource-constrained countries.**	DOJ and DOS, coordinate with international equivalents	30 days, ongoing

🟦 TANGIBLE ACTION UNDERWAY   🟩 PRELIMINARY ACTION NOTED   ⬜ NO KNOWN ACTION

MAY 2020

GOAL 2: DISRUPT THE RANSOMWARE BUSINESS MODEL

Objective		Rec.	Description	Lead	Timeline
Disrupt the system that facilitates the payment of ransoms	🟩	2.1.1	**Develop new levers for voluntary sharing of cryptocurrency payment indicators.**	Congress, CISA, international equivalents	6-12 months
	🟩	2.1.2	**Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws.**	U.S. Treasury, SEC, international equivalents	12 months
	🟩	2.1.3	**Incentivize voluntary information sharing between cryptocurrency entities and law enforcement**	U.S. Treasury (FinCEN)	12 months
	🟩	2.1.4	**Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.**	U.S. DOJ and international equivalents	6-12 months
	🟩	2.1.5	**Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation.**	U.S. and international insurance and re-insurance firms	6-12 months
	🟦	2.1.6	**Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs.**	SEC and international equivalents	6-12 months
	🟩	2.1.7	**Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.**	U.S. and international insurance and re-insurance firms	6-12 months (to establish consortium and initial subrogation effort)
Target the infrastructure used by ransomware criminals	🟩	2.2.1	**Leverage the global network of ransomware investigation hubs.**	USG and international equivalents	6-12 months
	⬜	2.2.2	**Clarify lawful defensive measures that private-sector actors can take when countering ransomware.**	Congress	12-24 months
Substantially reduce safe havens where ransomware actors currently operate with impunity	🟩	2.3.1	**Increase government sharing of ransomware intelligence.**	DHS	6 months, ongoing
	🟩	2.3.2	**Create target decks of ransomware developers, criminal affiliates, and ransomware variants.**	USG and national governments	6-12 months
	🟦	2.3.3	**Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure.**	U.S. law enforcement and international equivalents	12-24 months

🟦 **TANGIBLE ACTION UNDERWAY** 🟩 **PRELIMINARY ACTION NOTED** ⬜ **NO KNOWN ACTION**

MAY 2020

GOAL 3: HELP ORGANIZATIONS PREPARE

Objective	Rec.	Description	Lead	Timeline
Support organizations with developing practical operational capabilities	🟦 3.1.1	**Develop a clear, actionable framework for ransomware mitigation, response, and recovery.**	NIST, int'l equivalents, private sector participation	12-24 months, updated yearly thereafter
	🟩 3.1.2	**Develop complementary materials to support widespread adoption of the Ransomware Framework.**	NIST and international equivalents	12-24 months, updated regularly thereafter
	🟩 3.1.3	**Highlight available internet resources to decrease confusion and complexity.**	Internet search companies, along with nonprofit input	6-12 months for first iteration, ongoing thereafter
Increase knowledge and prioritization among organizational leaders	🟩 3.2.1	**Develop business-level materials oriented toward organizational leaders.**	CISA	6-12 months, with updates yearly as needed
	🟩 3.2.2	**Run nationwide, government- backed awareness campaigns and tabletop exercises.**	USG and int'l equivalents, appropriate agency leads, organizational partners	12-24 months, ongoing for as long as relevant
Update existing, or introduce new, cybersecurity regulations to address ransomware	🟦 3.3.1	**Update cyber-hygiene regulations and standards.**	State/Federal governments; support from state/local entities	Likely 12-24 months, with subsequent iterations
	🟩 3.3.2	**Require local governments to adopt limited baseline security measures.**	USG and international equivalents	6-12 months, updated yearly thereafter
	⬜ 3.3.3	**Require managed service providers to adopt and provide baseline security measures.**	Congress and international legislatures	6-12 months
Financially incentivize adoption of ransomware mitigations	🟩 3.4.1	**Highlight ransomware as a priority in existing funding provisions.**	Relevant fund designation agencies	3-6 months
	🟩 3.4.2	**Expand Homeland Security Preparedness Grants to encompass cybersecurity threats.**	DHS working with Congress	6-12 months
	🟩 3.4.3	**Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework.**	USG and international equivalents	Likely 12-24 months
	🟩 3.4.4	**Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.**	USG and international equivalents	12-24 months
	⬜ 3.4.5	**Investigate tax breaks as an incentive for organizations to adopt secure IT services.**	USG and international equivalents	24 months

🟦 TANGIBLE ACTION UNDERWAY   🟩 PRELIMINARY ACTION NOTED   ⬜ NO KNOWN ACTION

MAY 2020

GOAL 4: RESPOND TO RANSOMWARE ATTACKS

Objective	Rec.	Description	Lead	Timeline
Increase support for ransomware victims	🟩 4.1.1	**Create ransomware emergency response authorities.**	USG and international equivalents	12-24 months
	🟦 4.1.2	**Create a Ransomware Response Fund to support victims in refusing to make ransomware payments.**	USG, insurance industry	12-24 months
	🟩 4.1.3	**Increase government resources available to help the private sector respond to ransomware attacks.**	USG and international equivalents	12-24 months
	🟩 4.1.4	**Clarify United States Treasury guidance regarding ransomware payments.**	US Treasury	6-12 months
Increase the quality and volume of information about ransomware incidents	🟩 4.2.1	**Establish a Ransomware Incident Response Network (RIRN).**	A nonprofit and international equivalents	12-24 months to reach full operational capacity
	🟩 4.2.2	**Create a standard format for ransomware incident reporting.**	A nonprofit and international equivalents	6-12 months
	🟩 4.2.3	**Encourage organizations to report ransomware incidents.**	DHS/CISA	6-12 months, ongoing as needed
	🟩 4.2.4	**Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.**	USG and international equivalents	12-24 months
Require organizations to consider alternatives to paying ransoms	⬜ 4.3.1	**Require organizations to review alternatives before making payments.**	USG and international equivalents	12-24 months
	⬜ 4.3.2	**Require organizations to conduct a cost-benefit assessment prior to making a ransom payment.**	USG and international equivalents	12-24 months
	⬜ 4.3.3	**Develop a standard cost-benefit analysis matrix.**	NIST and international equivalents, private sector participation	12-24 months

🟦 TANGIBLE ACTION UNDERWAY 🟩 PRELIMINARY ACTION NOTED ⬜ NO KNOWN ACTION

MAY 2020

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org