Testimony of

Christopher C. Krebs

Before the

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

U.S. House of Representatives

On

Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis

May 5, 2021
Washington, DC

Via Cisco Webex

Testimony of Christopher C. Krebs
U.S. House of Representatives, Committee on Homeland Security
May 5, 2021

Introduction

Chairwoman Clark, Ranking Member Garbarino, Members of the Subcommittee, it is my pleasure to appear before you today to discuss much needed efforts to combat ransomware. My name is Christopher Krebs and I previously served as the first Director of the Cybersecurity and Infrastructure Security Agency (CISA), leading CISA and its predecessor organization, the National Protection and Programs Directorate, from August 2017 until November 2020. Over the last several years, I have had the pleasure of working with many of you as members of the primary oversight Committee for CISA and have testified in front of the committee several times.

It is an honor to appear before this Subcommittee to testify about the threat ransomware poses to countless organizations across this nation. Given my recent experience as CISA Director, and now as Founding Partner of the Krebs Stamos Group, a cybersecurity risk management consultancy, as well as the Newmark Senior Cyber Fellow at the Aspen Institute, I am continuing my commitment to improving the Nation's cybersecurity and resilience.

In 2011, famed Silicon Valley innovator and entrepreneur Marc Andreessen famously penned in a Wall Street Journal piece that "software is eating the world.[1]" A decade later, cyber criminals in the form of ransomware gangs have come around for their piece of the action. Considered a low-dollar, online nuisance crime only a few short years ago, ransomware has exploded into a multi-billion-dollar global racket that threatens the delivery of the very services so critical to helping us collectively get through the COVID pandemic. To put it simply, we are on the cusp of a global pandemic of a different variety, driven by greed, an avoidably vulnerable digital ecosystem, and an ever-widening criminal enterprise.

As we have spent the last several months debating appropriate responses to Russian and Chinese cyber activities, cyber operations that most Americans will not see any direct impact, ransomware, on the other hand, has continued to affect our communities. According to the 2020 Verizon Data Breach Report, Ransomware accounts for 27% of malware incidents, with the highest rate of occurrence in the education, healthcare, and government administration sectors[2].

Cybercriminals have been allowed to run amok while governments have mainly watched from the sidelines, unclear on whether cybercrime is a national security level threat. If there was any remaining doubt on that front, let's dispense with it now: too many lives are at stake. We need a different approach, and that shift is needed now. We have risen to the challenge in the past and can do it again.

[1] Marc Andreessen on Why Software Is Eating the World - WSJ
[2] 2021 Verizon Data Breach Report, Figure 5., pg 7. Available for download here.

The Context for the Ransomware Explosion

The underlying enabling factors for this cybercrime explosion are rooted in the digital dumpster fire of our seemingly pathological need to connect everything to the internet combined with how hard it is to actually secure what we have connected. Two more recent factors have thrown fuel on the already smoldering heap: the spread of cryptocurrencies that enable the transfer of funds largely outside the eyes of financial regulators, and corrupt safe havens that don't mind if a little crime happens on their turf as long as it brings home some revenue, directs malicious online activities elsewhere, and has the added benefit of making life more difficult for strategic adversaries.

It is important to reinforce that cryptocurrency in and of itself is not a criminal enterprise, nor do I think eradicating or regulating it to the point of uselessness is the answer. Like many other transformational technology developments, cryptocurrency has likely crossed a threshold where it is here to stay. In fact, in many markets, cryptocurrency and similar financial technology developments represent a promising future for technological innovation. Therefore, the challenge is to appropriately intervene to avoid societal harms while fostering a marketplace for technologies like cryptocurrency where we can both lead in innovation and maintain a globally competitive edge.

Even if software and services were more secure, the allure of a quick buck and no real repercussions means the forward-looking prospects for ransomware actors are quite good. But we do not even have good metrics on how good the market is, as there's no real clearinghouse of authoritative sources of information on the number of victims there are. The best source in fact may be to just ask the criminals themselves (and I'm not going to take their word for it) - they'll likely offer you cyber hygiene and security advice in their response.

Ransomware crews have been propelled and professionalized by commodity malware and specialization across various hacking techniques. The sophistication of the actors is impressive – it is not just a single gang running entire operations. Different groups of criminals have developed focused capabilities or access in different aspects of the heist and collaborate as they see fit to get the job done. This allows for a commoditization of the "kill chain," creating further opportunities to elude law enforcement and dance around international financial rules and regulations.

And while these gangs have become more sophisticated, governments have been sluggish in responding in a meaningful way. As a result, victims are often left to fend for themselves, turning to specialty incident response firms that have developed a niche industry for negotiating decryption. The costs of lost productivity, disrupted operations, inefficiency in markets, and operational recovery likely far outweigh the dollars siphoned out of the world's economies and dumped into illicit activities from human trafficking to the development of weapons of mass destruction. That's right - this malware has afforded Kim Jung Un's ability to continue to expand his nuclear arsenal. How is this still only viewed as a cybercrime?

For a few years, I have been stumping for a more coordinated approach across industry and government that can bring defenders together, break the payment chain, and put some

consequences on the bad guys either directly or have their landlords do it. But much like countering disinformation (and frankly cybersecurity in general), because of the cross-cutting nature of the problem, spanning different government agencies with different authorities, with often competing priorities and mission sets, national governments to include the United States have struggled to make meaningful progress.

Confronting the Growing Ransomware National Emergency

We have seen some glimpses of appetite to address the ransomware crisis with the recent announcement of the Department of Justice (DOJ) ransomware-focused initiative, and the Department of Homeland Security's ransomware 60-day sprint. This builds on efforts by the United States Secret Service, the Federal Bureau of Investigation (FBI), CISA, industry efforts like the National Cyber Forensics and Training Alliance, among others. Critically, there are indications that the White House is considering a more strategic approach on the ransomware front soon.

Ultimately, whatever the Administration and Congress choses to do, there is no single solution or silver bullet. No one agency alone will solve this problem. Much like confronting election security threats or disinformation more broadly, there are a range of levers that government and industry can pull to achieve positive outcomes. And there are past successes in operational collaboration that can be built on to ensure future success. For example, drawing on the lessons learned from the Russian efforts to interfere in the 2016 election, a coalition of agencies, including CISA, the National Security Agency (NSA), the FBI, and others, built a playbook that first prioritized effective coordination across Federal, state, and local government agencies. Second, increasing federal support and resources to election security stakeholders to improve defenses and response. And third, engaging the adversary to learn more about their operations but also disrupt activities where possible.

The secret sauce to our election security efforts were the clear acknowledgement that multiple agencies had the ability to contribute to the ultimate outcome and we all recognized that the greater good was more important than any individual agency's "turf" concerns. The U.S. along with our allies need to take a new, more strategic and coordinated approach to overcoming the emerging national security emergency posed by ransomware. Similarly, the counter ransomware "triplet" includes improving cyber defenses, disrupting the criminals' business model, and increased coordinated action against ransomware gangs and their enablers. This strategy will require government and the private sector to contribute and commit to partnering together to break the ransomware cycle.

Improving Defenses

First, we must improve defenses of our businesses and agencies across all levels of government. Ubiquitous use of multifactor authentication (MFA) for access to networks can limit credential abuse, updated and patched systems can prevent actors from exploiting known vulnerabilities, and a well-practiced incident response plan accompanied by backed up and

offline systems can enable rapid reaction and restoration. In many cases, even these straightforward steps are beyond the reach of many companies or state or local agencies. We need to rethink both our approach to technology deployment, including MFA by default, and the Federal government should consider increasing technology upgrade grants to states and localities to retire legacy systems and join the digital transformation.

Disrupting the Ransomware Business Model

Second, we must break the business model of ransomware. Simply put, ransomware is a business, and business is good. The criminals do the crimes and their victims pay the ransom. Often it seems easier (and seemingly the right thing to do from a fiduciary duty to shareholders perspective) to pay and get the decryption key rather than rebuild the network. There are three problems with this logic: (1) you are doing business with a criminal and expecting them to live up to their side of the bargain. It is not unusual for the decryption key to not work. (2) There is no honor amongst thieves and no guarantee that the actor will not remain embedded in the victim's network for a return visit later, after all the victim has already painted themselves an easy mark. (3) By paying the ransom, the victim is validating the business model and essentially making a capital contribution to the criminal, allowing them to hire more developers, more customer service, and upgrade delivery infrastructure. And, most worrisome, go on to the next victim.

We must address the ransomware business model head on and disrupt the ability of victims to pay ransom. We need to prioritize countering ransomware as a nation. That includes appropriately investing in our government agencies and their ability to investigate, disrupt, and apprehend criminals. We need to do more to understand the ransomware economy and the various players in the market. And at the points where cryptocurrency intersects with the traditional economy, we need to take action to provide more information, more transparency, and comply with the laws that are already on the books. This includes Kiosks, Over the Counter trading desks, and cryptocurrency. Lastly, we don't know enough about the ransomware economy, as it operates in the shadows. We lack a clear understanding of the scale of the problem, including the number of victims of ransomware – the denominator we aree trying to improve against.

There are different ways to do gain better insight into the ransomware economy, including requiring anyone paying a ransom (as a last resort, of course) to notify the government and provide specific details. There is an alternate model, where to make a payment to an identified (in this case an officially sanctioned organization) victims or their agents must seek a license or similar permission from the government prior to making that payment. The Department of Treasury Office of Foreign Asset Control (OFAC) began down this track last year, declaring ransom payments to identified entities may be a violation of economic sanctions laws. Because the identity of the ransomware actor is not always obvious, the OFAC advisory may have an overall chilling effect on ransom payments.

More Aggressive Action Against Ransomware Actors

Third, we need more coordinated action against ransomware actors using the range of authorities available to federal agencies, as well as capabilities and rights resident in the private sector. To be clear, I am not suggesting extrajudicial kinetic actions against ransomware gangs. However, other authorities available to law enforcement and military should be on the table, with great care taken not to blur the lines between the two. Traditional approaches have clearly not been sufficient to prevent the outbreak of ransomware. More aggressive and repeated disruption of malware command and control infrastructure, like the action earlier this year against *Emotet*, is a good start[3]. Where there are clear ties between ransomware actors and state actors or a potential imminent threat to an event or infrastructure of significance like a national election, action should be on the table. The private sector also has options available, as demonstrated by Microsoft's aggressive policing the abuse of its trademark and source code, including last fall's operation against *Trickbot*[4]. When coordinated and jointly conducted, private and public sector can make the internet an inhospitable place for cybercriminals.

Collective Action Against Ransomware

Last week was perhaps the most promising development in the fight against ransomware, with the Ransomware Task Force releasing its report[5]. The Task Force, a collaboration of more than 60 experts in cyber policy, software engineering, and academia, lays out a comprehensive set of recommendations that all players in the IT ecosystem can take. The report is 81 pages packed with evidence, analysis, and practical/actionable recommendations. It's clear that they've identified where the real policy and operational gaps lie: the need for prioritization across the national security structure, for greater ransomware-focused operational public-private collaboration, chokepoints in the crypto payments kill chain, and in addressing the challenges facing the cyber insurance industry.

Perhaps most importantly, the report calls for a coordinated strategy with real leadership from government and industry. This is a critical step forward – a clear commitment to lead from the front, to ensure the various agencies and actors are working in concert. It's not just enough for the government to coordinate itself, it needs to coordinate priorities, actions, and investments with the private sector. These actions can include taking disruptive steps against cybercriminals. Ultimately, the attack surface is not the federal.

The RTF also calls for standing up an international coalition, something that has existed principally in law enforcement channels, and should fold in defensive teams as well as intelligence agencies. We have shown time and time again that information sharing is most effective when the people that can act on the information – regardless of whether they are in industry or in government – actually have that information.

[3] Emotet Botnet Disrupted in International Cyber Operation | OPA | Department of Justice
[4] New action to combat ransomware ahead of U.S. elections - Microsoft On the Issues
[5] Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (securityandtechnology.org)

The RTF, importantly, calls for additional support to businesses and government agencies preyed on by ransomware actors. This support necessarily includes boosting preventative measures, but also sets out a set of actions that everyone can take to help victims work through an attack, and only as a last resort make payments, and even in such an undesirable event, requiring reporting and tracking. Maybe then we will get good sense of how big this problem really is and more effectively build out the tools that are needed to respond on the timescales these criminals operate on. If the U.S. Treasury is expected to facilitate incident reporting, identify suspicious activity, coordinate with law enforcement, and assist private sector victims all within the window of the extortion threat, they deserve the tools and resources they need to move with that kind of agility and speed. The same goes with the FBI and DOJ officers tasked with executing court orders to seize crypto wallets, or the team at CISA helping coordinate, respond, or work with State and Local authorities in advance to better defend their networks. Without these additional tools and resources, the criminals will continue to exploit these seams with impunity.

Lastly, for the RTF's recommendations to really take hold, the Administration and Congress need to start putting together a legislative package to enable the additional authorities and appropriations recommended by the group. Again, there is a clear roadmap for cyber-related law, recently trail blazed by the Cyberspace Solarium Commission, another group that tackled thorny cyber problems and was able to get dozens of new cyber provisions passed into law. In fact, there are a range of recommendations that already fit well into options the Solarium is considering as it continues developing further legislative proposals.

The Ransomware Task Force should be commended for their work over the last four months. They showed initiative and commitment and have delivered an actionable roadmap for helping us get through our current digital crisis. We have tackled and overcome challenges as great as this before, we can do it again. I encourage the Administration to take the recommendations on board and implement quickly, together with private industry, and I similarly encourage the Congress to consider smart legislative action.

Increasing Funding for State and Local Government Agencies

Perhaps the area with the greatest need for government investment is not necessarily within the Federal government, but within our State and Local partners. I recently wrote an op-ed on this subject with a former CISA-colleague, Matt Masterson[6]. The idea is simple, we can reduce attack surface across State, local, tribal, and territorial government organizations in this country by investing in more modern, cloud-based systems. In doing so, we can improve citizen services for all Americans, create more tech jobs in our communities, and continue to invest in today's and tomorrow's technology innovators. No, we are not going to defend our way out of the ransomware problem, but we can close out many existing vulnerabilities, and gain additional benefits along the way. It is a way to defend against today's threats, while investing in a more secure tomorrow.

[6] Congress needs to help modernize our digital infrastructure | TheHill

As Congress considers and debates various infrastructure investment packages, I respectfully encourage consideration of cyber and technology specific funding. Everything we do these days in some way is somehow enabled by the technologies around us. Even as we have all made dramatic shifts in the way we see our friends and family, work, worship, and entertain ourselves in this new pandemic-era, the underlying infrastructure in our communities may struggle to keep up in the coming years. The difference between the haves and the have nots will be even starker, as many government agencies will see a reduction in tax revenues due to the economic impacts of COVID.

Conclusion

In this era of surging ransomware, modernizing state and local IT systems is not just good government — it is a national security imperative. Investment and support of state and local cyber infrastructure is an investment in our democracy, our judicial system, law enforcement, and the privacy and security of our citizens. Our adversaries allow cybercriminals and their own state-supported hackers to operate from their own sovereign territory, disrupting citizen services and stealing money and intellectual property from U.S. governments and businesses alike. It is time to step up and provide all partners inside and outside government with the support and resources they need to effectively defend themselves.

I would like to thank the committee for holding this timely hearing. I would also like to thank you for your leadership and support of CISA. I look forward to your questions.