EXPLAINER: No ransomware silver bullet, crooks out of reach

April 29 2021, by Frank Bajak

In this April 2, 2021, file photo, Washington Metropolitan Police Department chief Robert Contee speaks during a news conference in Washington. Political hand-wringing in Washington over Russia's hacking of federal agencies and meddling in U.S. politics has mostly overshadowed a worsening digital scourge with a far broader wallop: crippling and dispiriting extortionary ransomware attacks by cybercriminal mafias. All the while, ransomware gangsters have become more brazen and cocky as they put more and more lives and livelihoods at risk. This week, one syndicate threatened to make available to local criminal

gangs data they say they stole from the Washington, D.C., metro police on informants. (AP Photo/Alex Brandon)

Political hand-wringing in Washington over Russia's hacking of federal agencies and interference in U.S. politics has mostly overshadowed a worsening digital scourge with a far broader wallop: crippling and dispiriting extortionary ransomware attacks by cybercriminal mafias that mostly operate in foreign safe havens out of the reach of Western law enforcement.

Stricken in the United States alone last year were more than 100 federal, state and municipal agencies, upwards of 500 health care centers, 1,680 educational institutions and untold thousands of businesses, according to the cybersecurity firm Emsisoft. Dollar losses are in the tens of billions. Accurate numbers are elusive. Many victims shun reporting, fearing the reputational blight.

All the while, ransomware gangsters have become more brazen and cocky as they put more and more lives and livelihoods at risk. This week, one syndicate threatened to make available to local criminal gangs data they say they stole from the Washington, D.C., metro police on informants. Another recently offered to share data purloined from corporate victims with Wall Street inside traders. Cybercriminals have even reached out directly to people whose personal info was harvested from third parties to pressure victims to pay up.

"In general, the ransomware actors have gotten more bold and more ruthless," said Allan Liska, an analyst with the cybersecurity firm Recorded Future.

The U.S. government now deems ransomware a national security threat.

The Department of Justice has just created a task force to tackle it.

On Thursday, a public-private task force including Microsoft, Amazon, the National Governors Association, the FBI, Secret Service and Britain and Canada's elite crime agencies delivered to the White House an 81-page urgent action plan for an aggressive and comprehensive whole-of-government assault on ransomware, with Homeland Security Secretary Alejandro Mayorkas set to accompany them for a formal online launch at 1 p.m. EDT.

WHERE DID RANSOMWARE COME FROM? HOW DOES IT WORK?

The criminal syndicates that dominate the ransomware business are mostly Russian-speaking and operate with near impunity out of Russia and allied countries. They are a continuation and refinement—ransomware was barely a blip three years ago—of more than two decades of cyber-thieving that spammed, stole credit cards and identities and emptied bank accounts. The syndicates have grown in sophistication and skill, leveraging dark web forums to organize and recruit while hiding their identities and movements with tools like the Tor browser and cryptocurrencies that make payments—and their laundering—harder to track.

Ransomware scrambles a victim organization's data with encryption. The criminals leave instructions on infected computers for how to negotiate ransom payments and, once paid, provide software decryption keys.

Last year, ransomware crooks expanded into data-theft blackmail. Before triggering encryption, they quietly exfiltrate sensitive files and threaten to expose them publicly unless ransoms are paid. Victims who diligently backed up their networks as a hedge against ransomware now had to think twice about refusing to pay. At the end of 2019, only one

ransomware group had an extortion site online that would publish such files. Now more than two dozen do.

Victims who refuse to pay can incur costs that far exceed the ransoms they might have negotiated. It happened recently to the University of Vermont Health Network. It suffered an estimated $1.5 million a day in losses in the two months it took to recover. More than 5,000 hospital computers, their data scrambled into gibberish, had to be wiped clean and reconstituted from backed-up data.

The University of California-San Francisco, heavily involved in COVID-19 research, barely hesitated before paying. It gave the criminals $1.1 million last June. Manufacturers have been especially hard-hit this year, with ransoms of $50 million demanded of computer makers Acer and Quanta, a major supplier of Apple laptops.

HOW ARE THESE CRIMINALS ORGANIZED?

Some top ransomware criminals fancy themselves software service professionals. They take pride in their "customer service," providing "help desks" that assist paying victims in file decryption. And they tend to keep their word. They have brands to protect, after all.

"If they stick to their promises, future victims will be encouraged to pay up," Maurits Lucas, director of intelligence solutions at the cybersecurity firm Intel471, told a webinar earlier this year. "As a victim you actually know their reputation."

The business tends to be compartmentalized. An affiliate will identify, map out and infect targets, choose victims and deploy ransomware that is typically "rented" from a ransomware-as-a-service provider. The provider gets a cut of the payout, the affiliate normally taking more than three-quarters. Other subcontractors may also get a slice. That can

include the authors of the malware used to break into victim networks and the people running the so-called "bulletproof domains" behind which the ransomware gangs hide their "command-and-control" servers. Those servers manage the remote sowing of malware and data extraction ahead of activation, a stealthy process that can take weeks.

WHY DO RANSOMS KEEP CLIMBING? HOW CAN THEY BE STOPPED?

In Thursday's report, the task force says it would be wrong to try to ban ransom payments, largely because "ransomware attackers continue to find sectors and elements of society that are woefully underprepared for this style of attack."

The task force recognizes that paying up can be the only way for an afflicted business to avoid bankruptcy. Worse, the sophisticated cybercriminals often have done their research and know a victim's cybersecurity insurance coverage limit. They've been known to mention it in negotiations.

That degree of criminal savvy helped drive average ransom payments to more than $310,000 last year, up 171% from 2019, according to Palo Alto Networks, a task force member.

Not surprisingly, the still-young cyber-insurance industry is reeling. Premiums have gone up by 50% to 100% in the past year as ransomware became the No. 1 claim, said Michael Phillips, chief claims officer of Resilience Insurance and a co-chair of the task force. On average, cyber-insurance claim payouts can now exceed 70% of what is paid in premiums—prompting some insurers to drop this type of insurance altogether, industry reports show.

The multi-pronged response to ransomware proposed by the task force

will require the kind of concerted diplomatic, legal and law enforcement cooperation with key allies that the Trump administration shunned, displacing what the authors call the current "uncoordinated, disjointed" response.

"There is no silver bullet, but if we're going to shift the trajectory of this type of attack the U.S. government has got to get at this with some speed," said task force co-chair Philip Reiner, CEO of the nonprofit Institute for Security and Technology.

Ransomware developers and their affiliates should be named and shamed (they are not always easy to identify) and regimes that enable them punished with sanctions, the report urges.

It calls for mandatory disclosure of ransom payments and a federal "response fund" to provide financial assistance to victims—in hopes that, in many cases, it will prevent them from paying ransoms. And it wants stricter regulation of cryptocurrency markets to make it more difficult for criminals to launder ransomware proceeds.

The task force also calls for something potentially controversial: amending the U.S. Computer Fraud and Abuse Act to let private industry actively block or limit online criminal activity, including of botnets, the networks of hijacked zombie computers that ransomware criminals use to sow infections.

The odds of successfully stifling ransomware are high, the report's authors acknowledge: "The old adage that a cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day, has never been more true."