Ransomware persists even as high-profile attacks have slowed

December 18 2021, by Eric Tucker and Alan Suderman

Kenneth Trzaska, President of Lewis & Clark Community College, poses for a photo on the college's campus Dec. 15, 2021, in Godfrey, Ill. The small Illinois school canceled classes for days after a ransomware attack last month that knocked critical computer systems offline. Credit: AP Photo/Jeff Roberson

In the months since President Joe Biden warned Russia's Vladimir Putin

that he needed to crack down on ransomware gangs in his country, there hasn't been a massive attack like the one last May that resulted in gasoline shortages. But that's small comfort to Ken Trzaska.

Trzaska is president of Lewis & Clark Community College, a small Illinois school that canceled classes for days after a ransomware attack last month that knocked critical computer systems offline.

"That first day," Trzaska said, "I think all of us were probably up 20-plus hours, just moving through the process, trying to get our arms around what happened."

Even if the United States isn't currently enduring large-scale, front-page ransomware attacks on par with ones earlier this year that targeted the global meat supply or kept millions of Americans from filling their gas tanks, the problem hasn't disappeared. In fact, the attack on Trzaska's college was part of a barrage of lower-profile episodes that have upended the businesses, governments, schools and hospitals that were hit.

The college's ordeal reflects the challenges the Biden administration faces in stamping out the threat—and its uneven progress in doing so since ransomware became an urgent national security problem last spring.

U.S. officials have recaptured some ransom payments, cracked down on abuses of cryptocurrency, and made some arrests. Spy agencies have launched attacks against ransomware groups and the U.S. has pushed federal, state and local governments, as well as private industries, to boost protections.

Yet six months after Biden's admonitions to Putin, it's hard to tell whether hackers have eased up because of U.S. pressure. Smaller-scale

attacks continue, with ransomware criminals continuing to operate from Russia with seeming impunity. Administration officials have given conflicting assessments about whether Russia's behavior has changed since last summer. Further complicating matters, ransomware is no longer at the top of the U.S.-Russia agenda, with Washington focused on dissuading Putin from invading Ukraine.

The White House said in a statement that it was determined to "fight all ransomware" through its various tools but that the government's response depends on the severity of the attack.

"There are some that are law enforcement matters and others that are high impact, disruptive ransomware activity posing a direct national security threat that require other measures," the White House statement said.

Ransomware attacks—in which hackers lock up victims' data and demand exorbitant sums to return it—surfaced as a national security emergency for the administration after a May attack on Colonial Pipeline, which supplies nearly half the fuel consumed on the East Coast.

The attack prompted the company to halt operations, causing gas shortages for days, though it resumed service after paying more than $4 million in ransom. Soon after came an attack on meat processor JBS, which paid an $11 million ransom.

Biden met with Putin in June in Geneva, where he suggested critical infrastructure sectors should be "off limits" for ransomware and said the U.S. should know in six months to a year "whether we have a cybersecurity arrangement that begins to bring some order."

He reiterated the message in July, days after a major attack on a

software company, Kaseya, that affected hundreds of businesses, and said he expected Russia to take action on cybercriminals when the U.S. provides enough information to do so.

Since then, there have been some notable attacks from groups believed to be based in Russia, including against Sinclair Broadcast Group and the National Rifle Association, but none of the same consequence or impact of those from last spring or summer.

One reason may be increased U.S. government scrutiny, or fear of it.

The Biden administration in September sanctioned a Russia-based virtual currency exchange that officials say helped ransomware gangs launder funds. Last month, the Justice Department unsealed charges against a suspected Ukrainian ransomware operator who was arrested in Poland, and has recovered millions of dollars in ransom payments. Gen. Paul Nakasone, the head of U.S. Cyber Command, told The New York Times his agency has begun offensive operations against ransomware groups. The White House says that "whole-of-government" effort will continue.

"I think the ransomware folks, the ones conducting them, are stepping back like, 'Hey, if we do that, that's going to get the United States government coming after us offensively,'" Kevin Powers, security strategy adviser for cyber risk firm CyberSaint, said of attacks against critical infrastructure.

U.S. officials, meanwhile, have shared a small number of names of suspected ransomware operators with Russian officials, who have said they have started investigating, according to two people familiar with the matter who were not authorized to speak publicly.

It's unclear what Russia will do with those names, though Kremlin

spokesman Dmitry Peskov insisted the countries have been having a useful dialogue and said "a working mechanism has been established and is actually functioning."

It's also hard to measure the impact of individual arrests on the overall threat. Even as the suspected ransomware hacker awaits extradition to the U.S. following his arrest in Poland, another who was indicted by federal prosecutors was later reported by a British tabloid to be living comfortably in Russia and driving luxury cars.

Some are skeptical about attributing any drop-off in high-profile attacks to U.S. efforts.

"It could have just been a fluke," said Dmitri Alperovitch, former chief technology officer of the cybersecurity firm Crowdstrike. He said asking Russia to crack down on large-scale attacks won't work because "it's way too granular of a request to calibrate criminal activity they don't even fully control."

Top American officials have given conflicting answers about ransomware trends since Biden's discussions with Putin. Some FBI and Justice Department officials say they've seen no change in Russian behavior. National Cyber Director Chris Inglis said there's been a discernible decrease in attacks but that it was too soon to say why.

It's hard to quantify the number of attacks given the lack of baseline information and uneven reporting from victims, though the absence of disruptive incidents is an important marker for a White House trying to focus its attention on the most significant national security risks and catastrophic breaches.

Victims of ransomware attacks in the past few months have included hospitals, small businesses, colleges like Howard University—which

briefly took many of its systems offline after discovering a September attack—and Virginia's legislature.

The attack at Lewis & Clark, in Godfrey, Illinois, was discovered two days before Thanksgiving when the school's IT director detected suspicious activity and proactively took systems offline, said Trzaska, the president.

A ransom note from hackers demanded a payment, though Trzaska declined to reveal the sum or identify the culprits. Though many attacks come from hackers in Russia or Eastern Europe, some originate elsewhere.

With vital education systems affected, including email and the school's online learning platform, administrators canceled classes for days after the Thanksgiving break and communicated updates to students via social media and through a public alert system.

The college, which had backups on the majority of its servers, resumed operations this month.

The ordeal was daunting enough to inspire Trzaska and another college president who he says endured a similar experience to plan a cybersecurity panel.

"The stock quote from everyone," Trzaska said, "is not if it's going to happen but when it's going to happen."

profile.html