

“We need to up our game”—DHS cybersecurity director on Iran and ransomware

Enlarge / Christopher Krebs, director of the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency, at a recent Senate hearing. Krebs issued a warning earlier this week on a surge in Iranian state-sponsored “malicious cyber activity.”

Tom Williams/CQ Roll Call via Getty Images

reader comments

41 with 29 posters participating, including story author

Share this story

Last weekend, Cybersecurity and Infrastructure Security Agency Director Christopher Krebs issued a statement warning about elevated malicious Internet activity from state-sponsored actors in Iran. The notice corresponded to new warnings from private security research firms, including Recorded Future, of a surge in preparatory activity over the past three months by APT33, a threat group connected to the Iranian government and Iranian Revolutionary Guard Corps (IRGC, Iran’s military).

In an interview with Ars, Krebs explained that the reason for the warning went beyond that “regional activity”—attacks on Saudi Arabian companies and other organizations in the Persian Gulf and South Asia.

“Over the course of the last couple of weeks, and in particular last week I’d say, [the activity] became specifically directed,” he said. A “sense of the

community”—reports from US intelligence and other agencies, as well as private sector cybersecurity vendors—showed a significant leap in spear-phishing attacks connected to infrastructure associated with APT33 against targets in the US over the past week, Krebs said. “So you combine that increase in activity with a historic intentionality and demonstrated ability, after previous destructive campaigns, and it was time to make a statement and say, ‘Hey look, everybody, this is heating up. And politically it is also heating up... We need to step up our game.’”

Watching out for phishes

CISA is a very new agency within DHS created last year by Congress and charged with taking on domestic cybersecurity and critical infrastructure security activities. Formed out of the Department of Homeland Security’s National Protection and Programs Directorate and the US Computer Emergency Readiness Team, CISA has a wide mandate that includes efforts to coordinate protection of the security of US election systems and to help federal, state, and local agencies better secure themselves against other information security and infrastructure risks.

But CISA’s role is, outside of the federal government, largely advisory. The agency has cybersecurity advisors who work with major industry groups associated with critical infrastructure, of which election infrastructure is just a small part. As Krebs put it, the agency (including its US CERT component) is an “integrator” of information from multiple sources, including the Office of the Director of National Intelligence and the components of the intelligence community and private information security partners.

While Krebs’ statement warned of wiper attacks, he noted, “We haven’t seen any malicious payloads yet, but my primary concern was that this is more than just an uptick—this is a

dramatic increase in activity.” Previous spikes in activity have been associated with attacks, Krebs continued, “whether you’re talking about data deletion attacks, wiper attacks, or classic ransomware. And there has also been a pretty dramatic increase in ransomware activity in the US—now, I’m not attributing that to Iran, but the bigger trend I think, and this is kind of my sense of the community, is that ransomware attacks are on the rise.”

Both the Iranian malicious activities and ransomware attacks are largely dependent on exploiting the same sorts of security issues. Both rely largely on the same tactics: malicious attachments, stolen credentials, or brute-force credential attacks to gain a foothold on targeted networks, usually using readily available malware as a foothold to use those credentials to then move across a network.

When asked if the recent ransomware attacks on cities across the US (including three recent attacks in Florida with dramatically larger ransom demands) were indicative of a new, more targeted set of campaigns against US local governments, Krebs said that the attacks were likely not targeted—at least not initially.

“I still think these [ransomware campaigns] are fairly expansive efforts, where [the attackers] are initially scanning, looking for certain vulnerabilities, and when they find one that’s when they start to target,” he said. “Again, I’m not sure we have the information right now saying they were specifically targeted. There was probably a down-select on the bigger target that they had pulled a little extra on it based on what they found in initial scanning. But I think you’re right in that we’re seeing a change in the M.O.—they’re going for the higher payout.”

Those bigger payouts are in turn helping ransomware operators to further develop their capabilities, Krebs explained. “That money is going back into the business model to increase the

sophistication and the capabilities—these guys aren't just saying, 'Boom, I'm done,' and moving the arrow. These guys are investing in themselves; they're building their capabilities. They're highly sophisticated operations with things customer service. It's really, truly turning into a line of business."

We're going to need a bigger boat

That surging threat is, in many ways, just as big a threat as a state actor—if not larger—as more state and local agencies are affected. "That's where I think we've got a lot to do—work in the federal government, to state, local governments, and work in Congress," Krebs said. "What are we going to do here to make it harder for the bad guys to be successful? How are we going to shore up these systems, and do it in a way that is reasonable to the people that actually own the network to do it with their own resources with help from the federal government? So, we are engaging at the state and local level with governments."

In 2018, that engagement took the form of a ransomware awareness campaign, which Krebs said CISA was "reinvigorating over the summer." So far, there has been increased buy-in from state and local leaders—Mayor Muriel Bowser of Washington, DC, was with Krebs in Israel this week for the CyberWeek conference at Tel Aviv University, for instance.

But there are limits to what CISA can do—limits driven largely by manpower. "I need to be able to push more a dedicated focus of resources, and that starts with people," Krebs said. "It starts with [cybersecurity] advisors reaching out to state and local governments. What I would like to see is one of my cyber security advisors [CSAs] in every state capital, someone who maintains a direct relationship with state governments but also works with jurisdictions, whether that's city or county. Now we've got only about two dozen [CSAs], but they have to focus on private sector, not just state and local government."

The recent ransomware explosion is just the latest reason that additional manpower is needed around CISA. With 2020 around the corner, election security is another. "These coordinators, these state-focused coordinators, would work with election jurisdictions, too," Krebs said. "The demand is just off the charts for our help right now. We're not talking about getting in there and developing networks for them, we're talking about just basic awareness and helping them develop their strategies and roadmaps for investments."

Currently, doing that will require action from Congress—and so far, that has been a non-starter. Earlier this week, Republicans in the Senate blocked action on a bill intended to boost the investment in election infrastructure security.

Still, Krebs said, he and his agency will continue to advocate for that kind of an investment more broadly for state and local information security. "If Congress wants to down the road decide to have a stronger security grant program for state and local governments and help them build their investment justifications and figure out where to put that money, that's how I see our engagement playing out over the next couple years," Krebs said.

<https://arstechnica.com/?p=1529393>