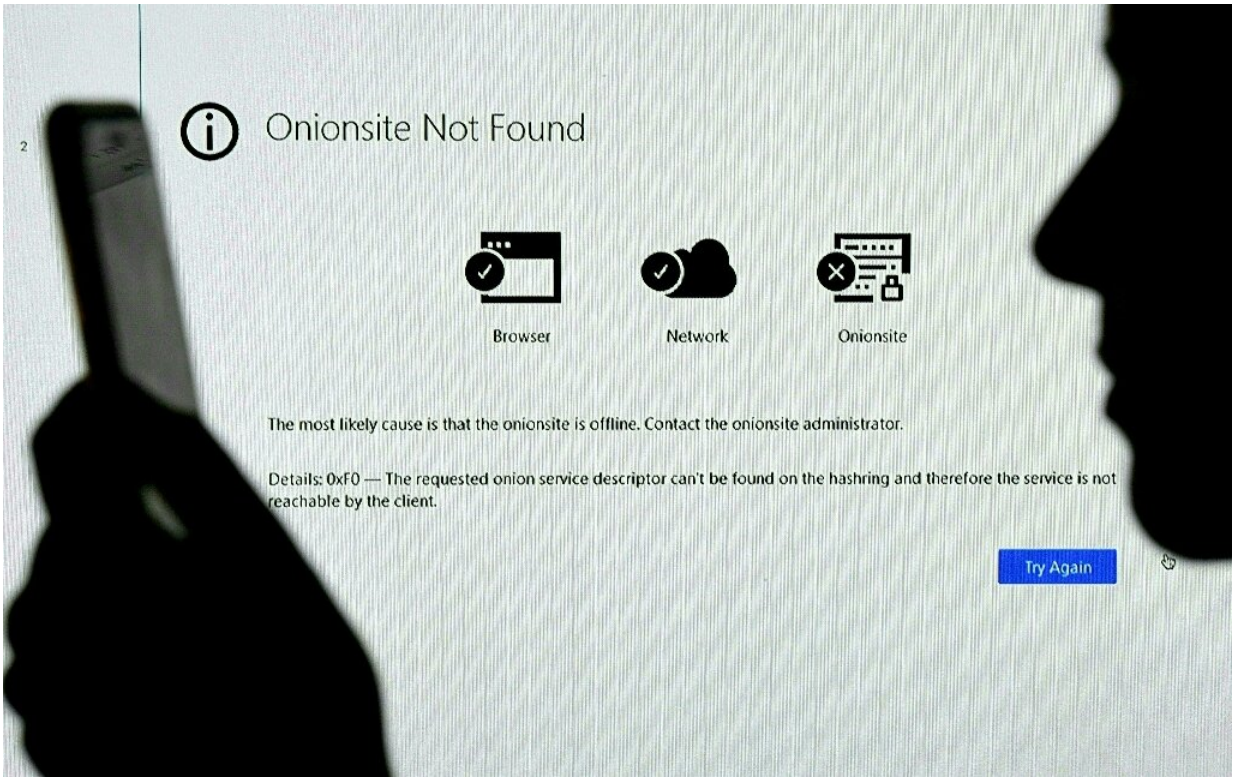
Tough fight looms against ransomware 'epidemic'

June 8 2021, by Rob Lever



An epidemic of ransomware has sparked calls for tougher action against hackers, with US officials pledging to make cyber investigations a top priority.

The latest wave of ransomware attacks hitting the United States and globally portends a difficult battle against hackers, even as government and the private sector ramp up defenses.

The attacks hitting the Colonial Pipeline and the major JBS meatpacking operations are examples of a burgeoning cybercrime industry with the potential to inflict pain and extract profits by impacting "critical" networks, experts say.

Other recent targets include local governments, hospitals, insurers, a ferry system and others in the United States and globally, with many of the attacks attributed to Russia-based hackers operating with at least tacit approval from the Kremlin.

At least $18 billion was paid to ransomware attackers last year, according to the security firm Emsisoft, which found "tens of thousands" of victims so far in 2021.

"Ransomware is hitting epidemic proportions and business as usual isn't going to cut it," said Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security.

Parham Eftekhari, chairman of the Institute for Critical Infrastructure Technology, a thinktank focused on cybersecurity, noted that a rush to digitization of more systems has opened up more avenues for hackers.

"We are prioritizing speed to market, functionality, profits and business objectives over security," Eftekhari said.

US officials in recent days have signaled a stepped-up effort on ransomware, calling these investigations a "top priority" and comparing the effort to the post-September 11 attacks fight against terror.

Covert US response

The Justice Department said Monday it recovered more than half of the $4.4 million ransom paid by Colonial Pipeline, in a rare success story.

Cybercriminals have been able to extract ransoms from victims in government and a variety of industries.

"The recovery of the ransom is, obviously, a positive as it signals to cybercriminals that their ill-gotten gains are not necessarily beyond the reach of law enforcement," said Brett Callow, analyst at the security firm Emsisoft.

But Callow said ransomware remains a scourge because "the financial rewards are huge (and) the chances of being caught are near-zero... we still have a very, very long way to go before the ransomware problem will be solved."

Following sanctions imposed on Moscow, US officials have said little about future responses, but analysts believe there is considerable activity under the radar.

"The US government appropriately responds sometimes in a covert manner," said Eftekhari.

"We have the greatest cyber offensive and defensive abilities on the planet."

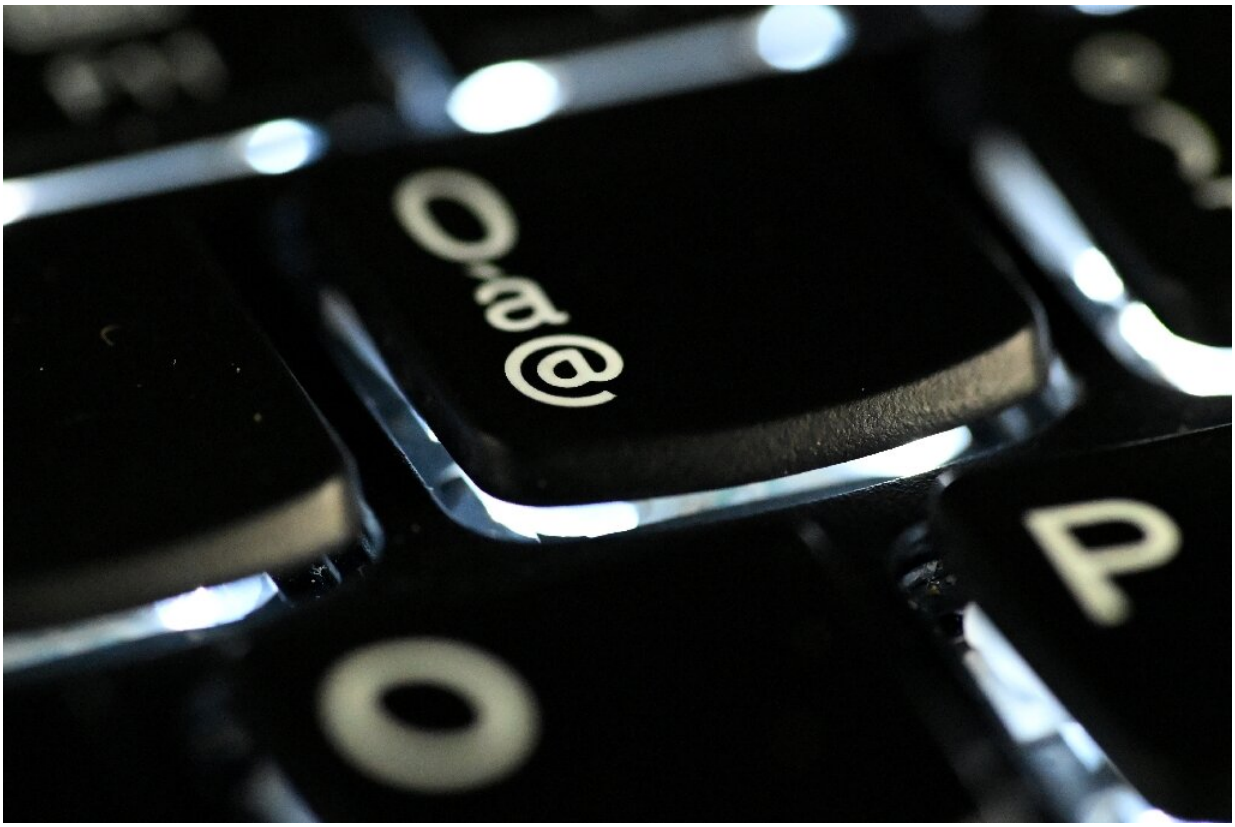
But security specialists say cyber defense is complex and requires actions across the board, including training for employees to avoid mistakes that let malicious actors into networks.

Security firm Proofpoint found in a recent survey that two-thirds of computer security officers acknowledge they are unprepared to cope with a future cyberattack, noted Proofpoint's Lucia Milica.

"Human error is one of the biggest vulnerabilities and we've seen that remote work has made networks more vulnerable," Milica said.

Line in the sand?

The latest attacks, on the heels of big data breaches affecting Microsoft email servers and the widely deployed SolarWinds security software, raise questions about protecting 16 "critical infrastructure" sectors including energy, utilities, defense, food and manufacturing.



Analysts see more cyberattacks coming without a concerted effort to improve security and prosecute hackers.

James Lewis, head of technology policy at the Center for Strategic and International Studies, said these sectors have been victimized frequently but that successes are obscured by high-profile hacks.

"We probably need to rethink what critical infrastructure is," Lewis said, suggesting that the label be used for public safety and national security.

Lewis said one lesson from the recent pipeline attack was panic buying of gasoline, which made the situation worse.

Making cryptocurrency transactions easier to trace could aid the fight

against ransomware by curbing anonymous transactions, some analysts say.

Lewis said this is a good idea but that "a more sophisticated approach would be for central banks to issue their own digital currencies, which could dry up the market for cryptocurrencies."

Cilluffo said the fight against ransomware will require a broad array of weapons.

"You really need to bring all instruments of power to bear: covert, diplomatic, military, sanctions," he said.

A summit next week with President Joe Biden and Russian counterpart Vladimir Putin offers a key moment for Washington to "draw a line" against Moscow for providing a haven for hackers, said Cilluffo.

"Cyber has to be items one, two and three," he said. "Having a president put markers in the silicon around cyber behavior is important because it comes with the full weight of the federal government."

Citation: Tough fight looms against ransomware 'epidemic' (2021, June 8) retrieved 25 March 2023 from https://techxplore.com/news/2021-06-tough-looms-ransomware-epidemic.html