The big Pentagon internet mystery now partially solved

April 25 2021, by Frank Bajak

This March 27, 2008, file photo, shows the Pentagon in Washington. After weeks of wonder by the networking community, the Pentagon has now provided a very terse explanation for why it hired a shadowy company residing at a shared workspace above a Florida bank to manage a colossal, previously idle chunk of the internet that it owns. Many basic questions remain unanswered, beginning with why it chose for the task a company that seems not to have existed until September. The company, Global Resource Systems, has not responded to attempts by The Associated Press to seek comment. (AP Photo/Charles Dharapak, File)

A very strange thing happened on the internet the day President Joe Biden was sworn in. A shadowy company residing at a shared workspace above a Florida bank announced to the world's computer networks that it was now managing a colossal, previously idle chunk of the internet owned by the U.S. Department of Defense.

That real estate has since more than quadrupled to 175 million addresses—about 1/25th the size of the current internet.

"It is massive. That is the biggest thing in the history of the internet," said Doug Madory, director of internet analysis at Kentik, a network operating company. It's also more than twice the size of the internet space actually used by the Pentagon.

After weeks of wonder by the networking community, the Pentagon has now provided a very terse explanation for what it's doing. But it has not answered many basic questions, beginning with why it chose to entrust management of the address space to a company that seems not to have existed until September.

The military hopes to "assess, evaluate and prevent unauthorized use of DoD IP address space," said a statement issued Friday by Brett Goldstein, chief of the Pentagon's Defense Digital Service, which is running the project. It also hopes to "identify potential vulnerabilities" as part of efforts to defend against cyber-intrusions by global adversaries, who are consistently infiltrating U.S. networks, sometimes operating from unused internet address blocks.

The statement did not specify whether the "pilot project" would involve outside contractors.

The Pentagon periodically contends with unauthorized squatting on its space, in part because there has been a shortage of first-generation

internet addresses since 2011; they now sell at auction for upwards of $25 each.

Madory said advertising the address space will make it easier to chase off squatters and allow the U.S. military to "collect a massive amount of background internet traffic for threat intelligence."

Some cybersecurity experts have speculated that the Pentagon may be using the newly advertised space to create "honeypots," machines set up with vulnerabilities to draw hackers. Or it could be looking to set up dedicated infrastructure—software and servers—to scour traffic for suspect activity.

"This greatly increases the space they could monitor," said Madory, who published a blog post on the matter Saturday.

What a Pentagon spokesman could not explain Saturday is why the Defense Department chose Global Resource Systems LLC, a company with no record of government contracts, to manage the address space.

"As to why the DoD would have done that I'm a little mystified, same as you," said Paul Vixie, an internet pioneer credited with designing its naming system and the CEO of Farsight Security.

The company did not return phone calls or emails from The Associated Press. It has no web presence, though it has the domain grscorp.com. Its name doesn't appear on the directory of its Plantation, Florida, domicile, and a receptionist drew a blank when an AP reporter asked for a company representative at the office earlier this month. She found its name on a tenant list and suggested trying email. Records show the company has not obtained a business license in Plantation.

Incorporated in Delaware and registered by a Beverly Hills lawyer,

Global Resource Systems LLC now manages more internet space than China Telecom, AT&T or Comcast.

The only name associated with it on the Florida business registry coincides with that of a man listed as recently as 2018 in Nevada corporate records as a managing member of a cybersecurity/internet surveillance equipment company called Packet Forensics. The company had nearly $40 million in publicly disclosed federal contracts over the past decade, with the FBI and the Pentagon's Defense Advanced Research Projects Agency among its customers.

That man, Raymond Saulino, is also listed as a principal in a company called Tidewater Laskin Associates, which was incorporated in 2018 and obtained an FCC license in April 2020. It shares the same Virginia Beach, Virginia, address—a UPS store—in corporate records as Packet Forensics. The two have different mailbox numbers. Calls to the number listed on the Tidewater Laskin FCC filing are answered by an automated service that offers four different options but doesn't connect callers with a single one, recycling all calls to the initial voice recording.

Saulino did not return phone calls seeking comment, and a longtime colleague at Packet Forensics, Rodney Joffe, said he believed Saulino was retired. Joffe, a cybersecurity luminary, declined further comment. Joffe is chief technical officer at Neustar Inc., which provides internet intelligence and services for major industries, including telecommunications and defense.

In 2011, Packet Forensics and Saulino, its spokesman, were featured in a Wired story because the company was selling an appliance to government agencies and law enforcement that let them spy on people's web browsing using forged security certificates.

The company continues to sell "lawful intercept" equipment, according

to its website. One of its current contracts with the Defense Advanced Research Projects Agency is for "harnessing autonomy for countering cyber-adversary systems." A contract description says it is investigating "technologies for conducting safe, nondisruptive, and effective active defense operations in cyberspace." Contract language from 2019 says the program would "investigate the feasibility of creating safe and reliable autonomous software agencies that can effectively counter malicious botnet implants and similar large-scale malware."

Deepening the mystery is Global Resource Systems' name. It is identical to that of a firm that independent internet fraud researcher Ron Guilmette says was sending out email spam using the very same internet routing identifier. It shut down more than a decade ago. All that differs is the type of company. This one's a limited liability corporation. The other was a corporation. Both used the same street address in Plantation, a suburb of Fort Lauderdale.

"It's deeply suspicious," said Guilmette, who unsuccessfully sued the previous incarnation of Global Resource Systems in 2006 for unfair business practices. Guilmette considers such masquerading, known as slip-streaming, a ham-handed tactic in this situation. "If they wanted to be more serious about hiding this they could have not used Ray Saulino and this suspicious name."

Guilmette and Madory were alerted to the mystery when network operators began inquiring about it on an email list in mid-March. But almost everyone involved didn't want to talk about it. Mike Leber, who owns Hurricane Electric, the internet backbone company handling the address blocks' traffic, didn't return emails or phone messages.

Despite an internet address crunch, the Pentagon—which created the internet—has shown no interest in selling any of its address space, and a Defense Department spokesman, Russell Goemaere, told the AP on

Saturday that none of the newly announced space has been sold.