Public Safety

Ransomware attacks increasing in Oregon, nationwide, FBI says

Updated: Jun. 30, 2022, 8:36 a.m. | Published: Jun. 30, 2022, 7:00 a.m.

Oregon's FBI cyber squad is one of the busiest units in the local FBI office, prompting Oregon's FBI Special Agent in

By Maxine Bernstein | The Oregonian/OregonLive

FBI agents with the bureau's Cyber Task Force in Oregon helped investigators identify three suspected Russian government hackers accused of compromising the computer network of a company that runs a nuclear power plant in Kansas.

The Portland-based FBI agents had expertise in the type of malicious software used to infect the operator of the Wolf Creek nuclear plant in Kansas.

Their work with FBI agents in Anchorage, Alaska, and bureau headquarters in Virginia led to federal indictments in Kansas of three men with ties to Russia's Federal Security Service, the principal security agency of Russia.

The case is just one example of the growing ransomware threat to vital U.S. industries, private companies and public agencies, the head of Oregon's FBI says.

Ransomware is malicious software that blocks access to a computer system or files until a "ransom" is paid.

Ransomware complaints to the FBI increased by 82% from 2019 to 2021, according to Kieran L. Ramsey, special agent in charge of Oregon's FBI.

Oregon's FBI cyber squad is one of the busiest units in the local FBI office, prompting Ramsey to redouble the office's efforts to sound the alarm about the pervasive threats. All of the FBI's 56 field offices have a cyber task force.

In Oregon in the past year, healthcare companies and school districts have been significant targets as well as more mom-and-pop shops and smaller businesses, such as Yoshida Foods and McMenamins.

The FBI has noticed not only a significant increase in the number of ransomware variants, but also in the number of attacks and the amount of money demanded, according to Ramsey. A variant is a type of encryption or hacking tool or code used to infiltrate a computer system, experts said.

In 2019, the FBI's global Internet Crime Complaint Center received 2,047 ransomware complaints, with losses of more than $8.9 million reported. In 2021, the center received 3,729 ransomware complaints with losses of more than $49.2 million.

The scams have grown in sophistication. The threats can come from people operating outside the United States who are trying to threaten national or economic security or from criminal groups driven by profit.

Criminal hackers also sometimes create a franchise system, contracting out their ransomware and hacking tools to other developers or for use by other nations, Ramsey said.

Sometimes, a double extortion occurs as victims are coerced into paying a ransom to have their data unlocked but also not to have it publicly leaked.

"That shows you the real-world threat to your business legitimacy because what's going to happen to your business when your customers and your shareholders see that your stuff is walking out the back door and being put on the internet for everybody," Ramsey said.

He wants the private and public sector -- particularly companies working in health care, banking, energy or transportation -- to be aware of the problem, reach out to the FBI ahead of time to form a partnership and contact the FBI right away if they detect an intrusion into their computer networks.

"The quicker they reach out to us, the better the chance that perhaps we can claw back some of that money" paid as ransom, he said.

How to deter cyberattacks

In the FBI's Portland field office, its Safe Streets Task Force investigating gun violence and its cyber task force are the two busiest squads in the building, Ramsey said. The cyber task force has more than a dozen data analysts, computer scientists, intelligence analysts, operations specialists and special agents.

They have familiarity with the more than 100 ransomware variants that have been detected globally. They also have formed private and government partnerships and fostered overseas partners that help with intelligence in investigating cyberattacks, he said.

The three alleged Russian government hackers accused in the Kansas case also are charged with conspiring to compromise critical infrastructure and energy companies worldwide from 2012 to November 2017.

They hid malware inside more than 17,000 software devices and controllers used by power and energy companies in the United States and elsewhere, according to a federal indictment. They are presumed to be in Russia and have not been arrested.

In Oregon, the Oregon Anesthesiology Group was the victim of ransomware on July 11, 2021, when it was locked out of its servers, according to the group. It alerted the FBI and a cyber forensics firm and were told federal agents had seized an account belonging to Ukrainian hackers.

The hackers had exploited a vulnerability in a third-party firewall, enabling them to gain entry to the Oregon company's network and figure out the administrator's credentials. Then they accessed names, addresses, dates of service, diagnosis, insurance provider names and IDS of 750,000 patients and 522 current and former employees, according to the company.

After the attack last year, the group replaced its third-party firewall and expanded use of multi-factor authentication to access its system. It also contracted with a vendor for around-the-clock security monitoring and increased use of cloud-based infrastructure, the group said in a statement.

In 2019, Portland Public Schools fell victim to a multimillion-dollar cyber scam after fraudsters tricked one or more employees through a compromised email account into wiring them money.

In such attacks, the offenders pose as a trusted staff member in an organization, such as a chief executive officer, with the legitimate bank accounts surreptitiously swapped with attacker-controlled ones.

The school district contacted the FBI immediately and expected to claw back about $2.9 million in district funds that had been transferred to a fraudulent account, with banks involved freezing the money transfer.

The FBI is continuing to investigate the school district breach, Ramsey said.

The FBI doesn't encourage paying a ransom because it may encourage the hackers to target additional organizations and doesn't guarantee a victim's files will be recovered, according to the agency.

Yet the FBI understands businesses that can't function may pay a ransom just to get back to work. But Ramsey said they should still report the attacks to the FBI local field office.

If contacted early, "we can either disrupt it or mitigate it...and prevent further harm from going forward," he said.

Darrin Johnson, leader of the cybersecurity team for the information technology company Progent, emphasized that hackers strike not only large companies but small- to medium-sized businesses.

A company's average ransom payment in the first quarter of 2022 in the U.S. was $211,259, he said.

The FBI has become more involved in fighting ransomware since 2019, but Johnson said those responsible are often beyond law enforcement's grasp.

Many live in countries that don't have extradition treaties with the United States and would face arrest only if they got caught after entering the U.S. or in another country with an extradition treaty, Johnson said.

"In some cases, we know exactly who the threat actors are," he said. "We know where it's coming from outside the country, and there's nothing we can do about it."

He also acknowledged that some companies avoid going to the FBI because they don't want anyone to know about the breach.

Still, he and Ramsey said, it's good to report the attacks, if only for sharing information.

"Chances are some other organization somewhere in the U.S. is at the same time, being victimized in the same way," Ramsey said.

-- Maxine Bernstein