Meet Babuk, a ransomware attacker blamed for the Serco breach

By Sean Lyngaas

Published: 2021-02-04 · Archived: 2026-04-05 17:49:57 UTC

It began with a laughable offer.

Someone calling themselves “biba99” on a popular criminal forum claimed on Jan. 5 to provide “non-malicious” software to help organizations identify “security issues.” The author struggled to explain, in halting English, “why we are not … criminals” while assuring readers that the group would not hack hospitals or schools.

A month later, the attacker behind what appeared to be a bumbling forum post is reportedly claiming responsibility for a ransomware attack on the multibillion-dollar outsourcing firm Serco.

The ransomware gang, dubbed Babuk after the strain of code it uses, is a case study in how quickly crooks can learn the basics of digital extortion — and how that breeds ambition for big corporate scalps. It shows how even relatively unsophisticated criminals can bedevil major corporations.

After claiming to only target companies that earn less than $4 million, the Babuk attacker went after Serco, Sky News reported on Sunday. The outsourcing firm reported more than $4 billion in revenue in 2019.

“Serco’s mainland European business has been subject to a cyber attack,” a Serco spokesperson said. “The attack was isolated to our continental European business, which accounts for less than 3% of our overall business. It has not impacted our other business or operations.”

The incident comes after security firms and insurers increasingly have emphasized that digital extortionists learn from other attackers’ techniques, outsource some of their operations and rely on connections to infiltrate victim networks.

“Like many actors new to the world of ransomware, the actor behind Babuk ransomware has been learning on the job while drawing insights from other criminal groups,” said Allan Liska, an intelligence analyst at the threat intelligence company Recorded Future.

“As they have completed attacks, they have taken lessons learned and incorporated them into the code,” Liska said. He pointed to how the attacker has included new features that ensure victim machines can be encrypted before the ransomware is deployed.

The Babuk attacker has also set up a website to pressure victims to pay — a common tactic among ransomware crooks.

The attacker has typically demanded $60,000 to $85,000 in ransoms, but that is “likely to increase over time as the threat actor becomes more experienced in ransomware operations,” according to a private analysis from PricewaterhouseCoopers obtained by CyberScoop.

Babuk is far from sophisticated. Its code has contained errors that kept it from executing on some targeted computers, according to PwC. “We assess that, due to a disregard for error checking, Babuk would fail to execute altogether in some environments,” the analysis says.

But while Babuk is still a relatively low-level threat to organizations, according to Liska, that could change if they are able to earn more money from attacks and invest in new capabilities.

“Efficacy breeds profit, which breeds capability in the ransomware business,” Liska said.
