Concerns grow as LockBit knockoffs increasingly target popular vulnerabilities

By Jonathan Greig

Published: 2023-10-19 · Archived: 2026-04-05 19:40:37 UTC

Hackers are using a leaked toolkit used to create do-it-yourself versions of the popular LockBit ransomware, making it easy for even amateur cybercriminals to target common vulnerabilities.

The LockBit ransomware gang, which has attacked thousands of organizations across the world, had the toolkit leaked in September 2022 by a disgruntled affiliate. Experts immediately expressed concerns that less-skilled hackers would be able to create their own ransomware with the tool.

Those fears have now been realized, according to researchers at Sophos, who have unveiled at least two instances in recent weeks where hackers exploiting popular vulnerabilities are using makeshift ransomware strains created from the builder to attack organizations.

Last week, Sophos reported seeing hackers attempting to exploit CVE-2023-40044 — a vulnerability affecting Progress Software's WS_FTP Server product. Progress disclosed the bug three weeks ago and released a patch for it, but Sophos said that it still found unpatched servers.

Christopher Budd, director of threat intelligence at Sophos, told Recorded Future News the only ransomware his team observed in these attacks were compiled from the LockBit builder leaked last year.

Sophos shared a copy of a ransom note purportedly from "The Reichsadler Cybercrime Group" that included a reference to the heraldic eagle image used by Nazi Germany and the Holy Roman Empire. The note demands the bitcoin equivalent of $500 from the would-be target.

Sean Gallagher, principal threat researcher at Sophos, told Recorded Future News on Thursday that they saw a second situation where hackers using a LockBit knockoff were attempting to attack outdated and unsupported Adobe ColdFusion servers.

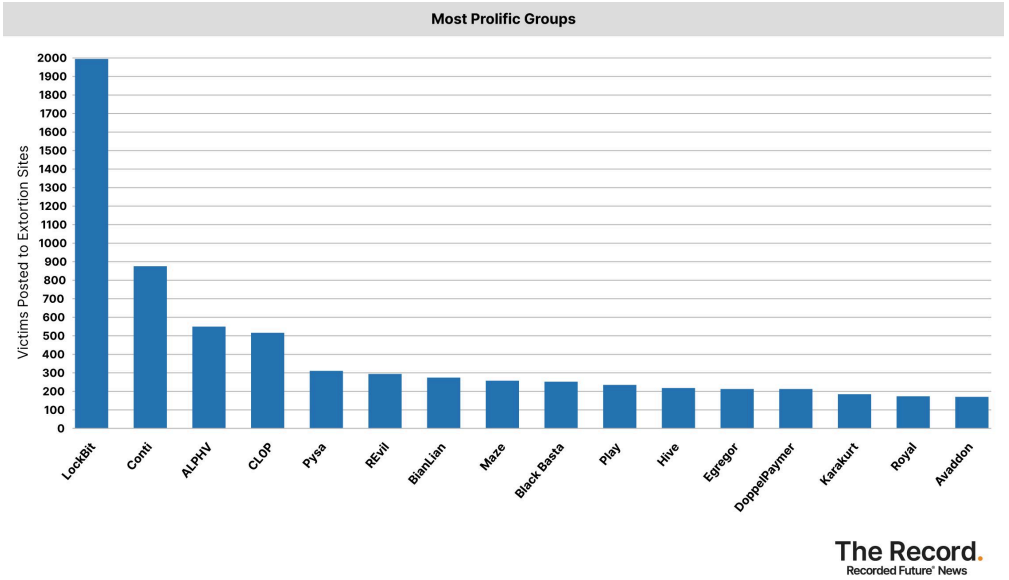
The hackers called the ransomware "BlackDogs2023" and Sophos said their systems were able to block the attack before it progressed. The ransom note from BlackDogs2023 requested 205 Monero (roughly $30,000) to recover the "stolen and encrypted" data.

"This is the second, recent incident of threat actors attempting to take advantage of leaked LockBit source code to spin new variants of ransomware that we've uncovered in recent weeks," he said.

"It's entirely possible that other copycats will emerge, which is why it's essential for organizations to prioritize patching and upgrading from unsupported software whenever possible. However, it's important to note that patching only closes the hole. With things like unprotected ColdFusion servers and WS_FTP, companies need to

also check to make sure none of their servers are already compromised, otherwise, they're still at risk of these attacks."

The leak of tools used to create ransomware strains has long been a concern of researchers, who noted that hundreds of strains can be traced back to a handful of popular ransomware brands.



Recorded Future ransomware expert Allan Liska said last year that his team identified more than 150 "new" ransomware groups, most of which are using code stolen from defunct ransomware gangs like Conti or REvil.

About one in every six ransomware attacks targeting U.S. government offices in 2022 were traced back to LockBit, according to June advisory from several U.S. law enforcement agencies. The gang has brought in about $91 million in ransoms from U.S. victims since its first reported attack in the country in January 2020.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
