BlackSuit ransomware extortion sites seized in Operation Checkmate

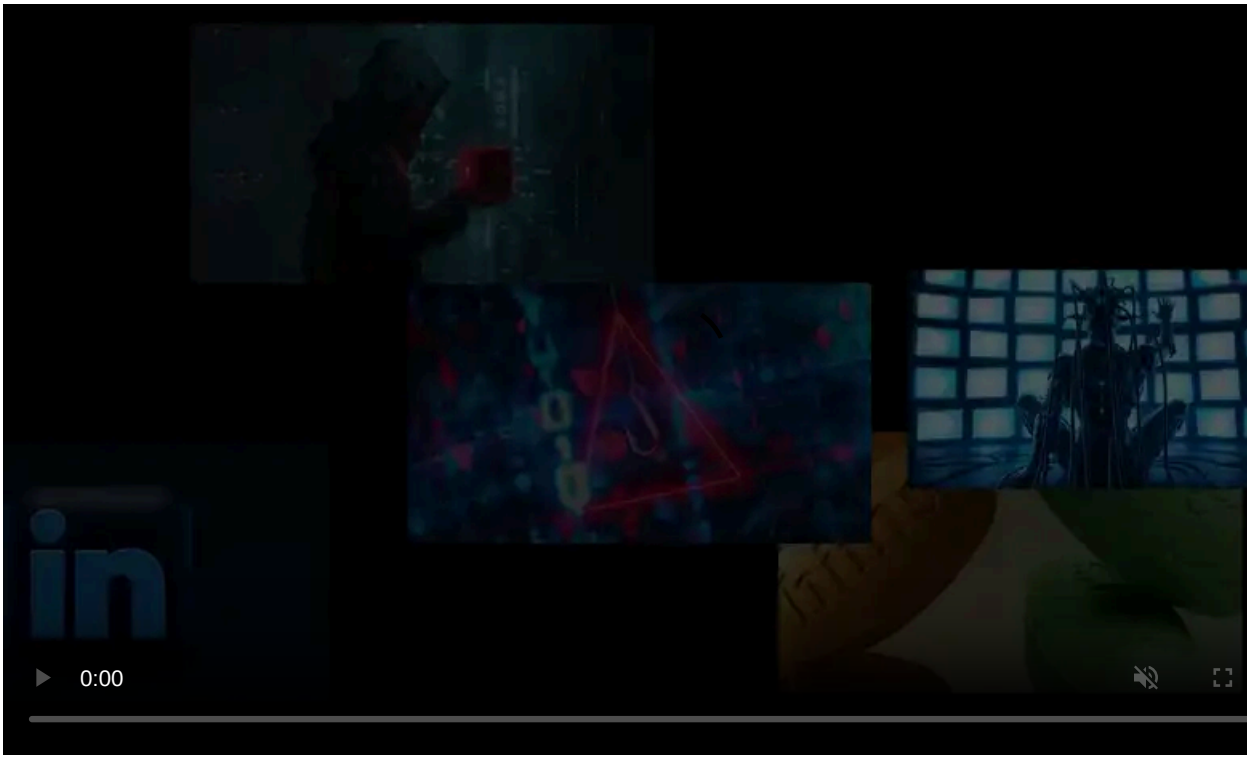
By Sergiu Gatlan

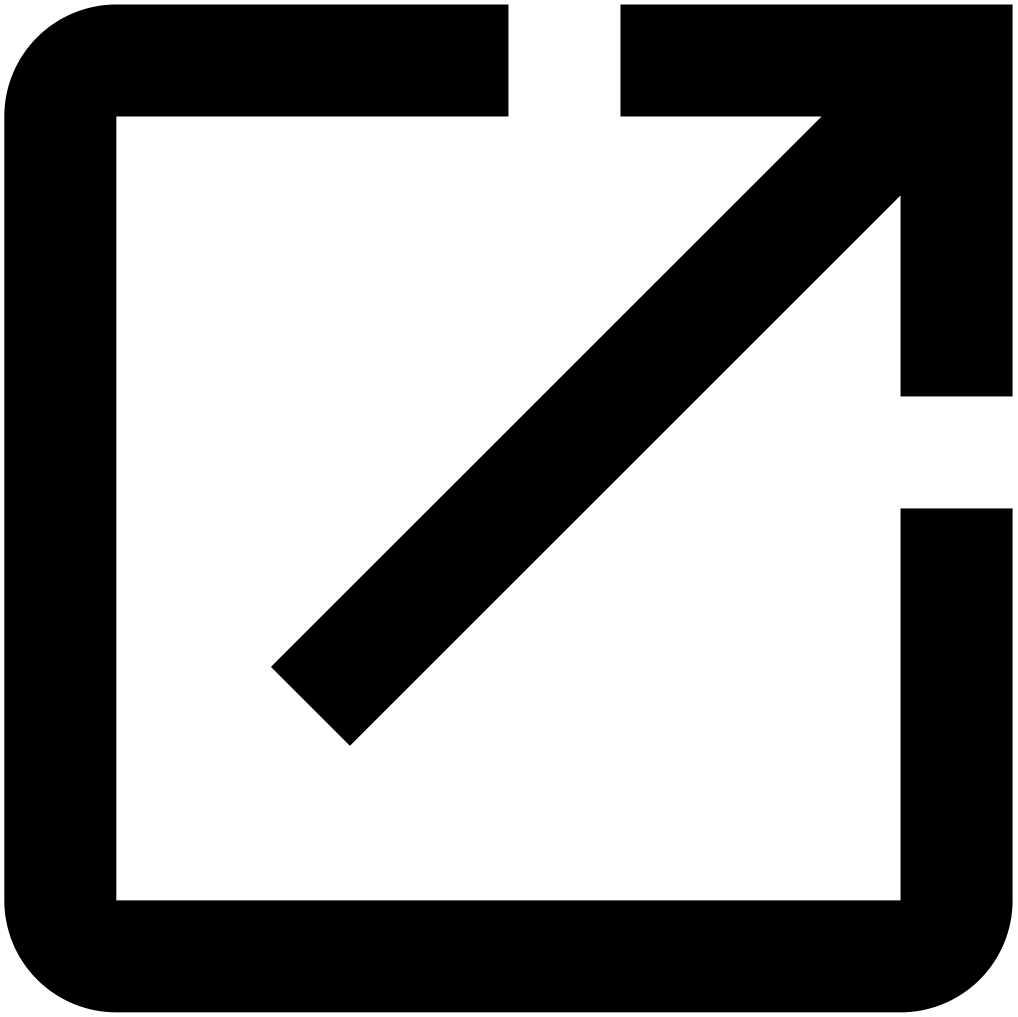
Published: 2025-07-24 · Archived: 2026-04-05 18:14:04 UTC

Law enforcement has seized the dark web extortion sites of the BlackSuit ransomware operation, which has targeted and breached the networks of hundreds of organizations worldwide over the past several years.

The U.S. Department of Justice confirmed the takedown in an email earlier today, saying the authorities involved in the action executed a court-authorized seizure of the BlackSuit domains.

Earlier today, the websites on the BlackSuit .onion domains were replaced with seizure banners announcing that the ransomware gang's sites were taken down by the U.S. Homeland Security Investigations federal law enforcement agency as part of a joint international action codenamed Operation Checkmate.


0:00



"This site has been seized by U.S. Homeland Security Investigations as part of a coordinated international law enforcement investigation," the banner reads.

BleepingComputer has confirmed that the seized sites include dark web data leak blogs and negotiation sites used to extort victims into paying ransom demands.

Other law enforcement authorities that participated in this joint operation include the U.S. Secret Service, the Dutch National Police, the German State Criminal Police Office, the U.K. National Crime Agency, the Frankfurt General Prosecutor's Office, the Justice Department, the Ukrainian Cyber Police, Europol, and others.

A spokesperson for Romanian cybersecurity company Bitdefender also told BleepingComputer that its cybercrime unit (known as Draco Team) provided cybersecurity consulting and guidance to law enforcement partners throughout Operation Checkmate.

"We commend our law enforcement partners for their coordination and determination. Operations like this reinforce the critical role of public-private partnerships in tracking, exposing, and ultimately dismantling ransomware groups that operate in the shadows," Bitdefender said.

BlackSuit seizure banner (BleepingComputer)

Chaos ransomware rebrand

On Thursday, the Cisco Talos threat intelligence research group reported that it had found evidence suggesting the BlackSuit ransomware gang is likely to rebrand itself once again as Chaos ransomware.

"Talos assesses with moderate confidence that the new Chaos ransomware group is either a rebranding of the BlackSuit (Royal) ransomware or operated by some of its former members," the researchers said.

"This assessment is based on the similarities in TTPs, including encryption commands, the theme and structure of the ransom note, and the use of LOLbins and RMM tools in their attacks."

BlackSuit started as Quantum ransomware in January 2022 and is believed to be a direct successor to the notorious Conti cybercrime syndicate. While they initially used encryptors from other gangs (such as ALPHV/BlackCat), they deployed their own Zeon encryptor soon after and rebranded as Royal ransomware in September 2022.

In June 2023, after targeting the City of Dallas, Texas, the Royal ransomware gang began working under the BlackSuit name, following the testing of a new encryptor called BlackSuit amid rumors of a rebranding.

CISA and the FBI first revealed in a November 2023 joint advisory that Royal and BlackSuit share similar tactics, while their encryptors exhibit obvious coding overlaps. The same advisory linked the Royal ransomware gang to attacks targeting over 350 organizations worldwide since September 2022, resulting in ransom demands exceeding $275 million.

The two agencies confirmed in August 2024 that the Royal ransomware had rebranded as BlackSuit and had demanded over $500 million from victims since surfacing more than two years prior.

Update 7/24/25: Updated article to include that negotiation sites were seized as well.

Source: https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/