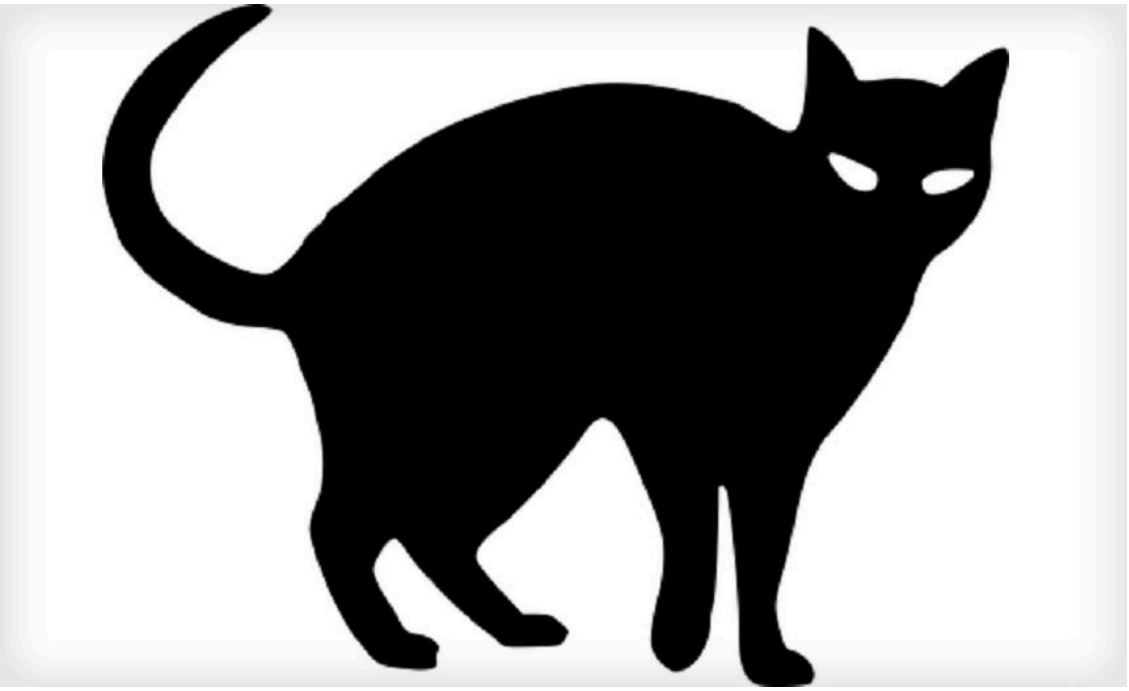
BlackCat Attacks University of Pisa, Demands $4.5M Ransom

By Mihir Bagwe

Archived: 2026-04-05 21:09:17 UTC

Critical Infrastructure Security , Cybercrime , Cybercrime as-a-service

Threat Actor Has Been Targeting the Education Sector in Europe and Elsewhere (MihirBagwe) • June 14, 2022



BlackCat ransomware appears to have claimed the University of Pisa as its latest victim.

See Also: AI Pushes Cyberattacks to New Speed Levels

Ransomware hackers reportedly seek a ransom of $4.5 million after seizing the university's IT system.

The threat actor says the ransom is a "discount price" that will increase to $5 million after Thursday, Cybersecurity360 reported. The Italian news site shared a screenshot of the alleged ransom note, which contains a clock counting down the minutes until the price jump.

The BlackCat ransomware-as-a-service group, which may be a rebrand of the DarkSide or BlackMatter ransomware groups, is also known as ALPHV. Its products are coded with Rust, a programing language known for fast performance and structural protections against some types of bugs. Analysis by cybersecurity firm Varonis shows the group actively recruiting operators with promises that affiliates can keep 90% of victims' payouts.

News of the attack comes days after the BlackCat ransomware group added the University of Pisa to its darknet list of victims, according to cybersecurity firm BetterCyber. The company adds that on Saturday, the threat group posted on its website: "Let's play, the University goes to sleep, the mafia wakes up?"

The University of Pisa did not respond to Information Security Media Group's request for comment.

On BlackCat's Target List: Educational Institutes

The University of Pisa, founded in 1343, wouldn't be the first academic institution to fall to BlackCat ransomware.

On June 2, BlackCat's victim list allegedly grew to include a French educational institute, the Ecole des Ingénieurs de la Ville de Paris.

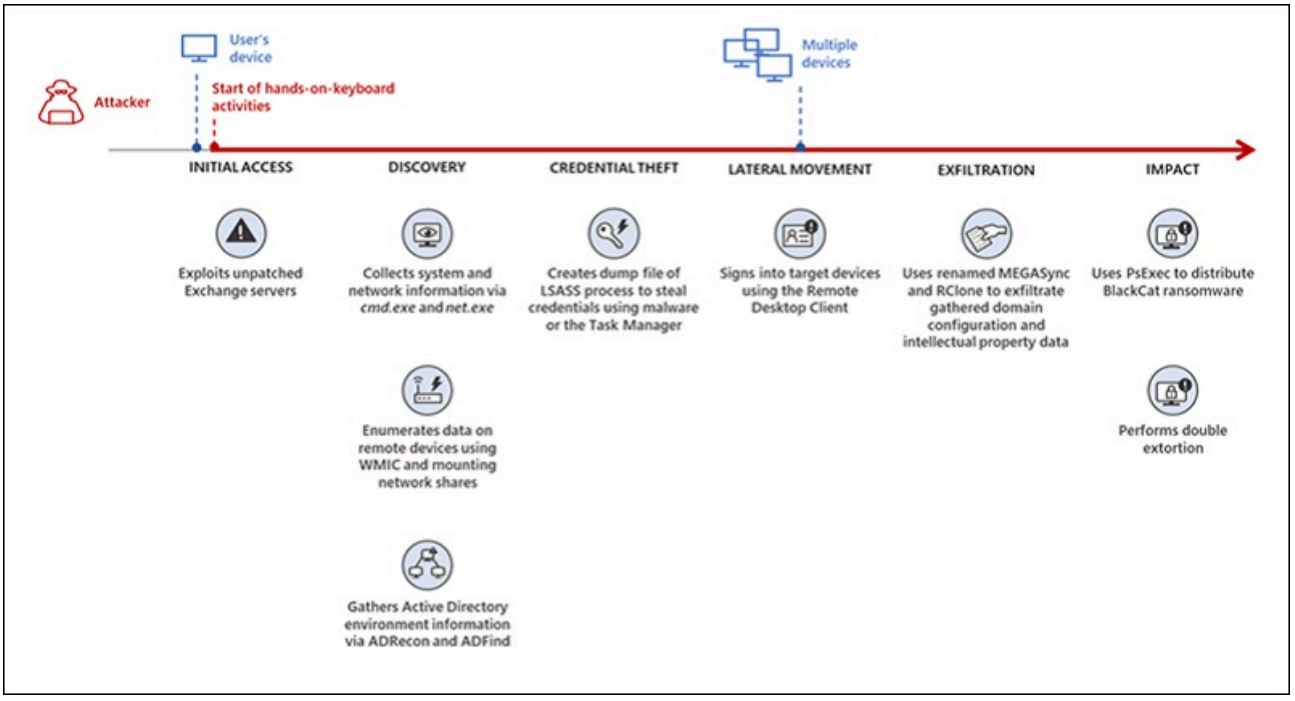
The ransomware group on its darknet website reportedly says it stole from the French institute more than 30 gigabytes worth of personally identifiable and financial information and other data protected by European privacy regulations.

Neither do European institutions stand alone. Among their North American cohorts are Florida International University, the North Carolina Agricultural and Technical State University, and a Canadian public school district in Saskatchewan. In Asia, Bangkok's Asian Institute of Technology also underwent a ransomware attack (see: *Update: What's BlackCat Ransomware Been Up to Recently?*).

New Attack Vector

BlackCat ransomware affiliates are leveraging unpatched Microsoft Exchange server vulnerabilities, according to a Monday post by the Microsoft 365 Defender Threat Intelligence team.

How BlackCat ransomware enters a target organization's network depends on the ransomware-as-a-service affiliate that deploys it, Microsoft researchers say. The most common method is via remote desktop applications and compromised credentials. But, "we also saw a threat actor leverage Exchange server vulnerabilities to gain target network access."



BlackCat ransomware attack chain via Exchange vulnerability exploitation (Source: Microsoft)

Microsoft did not specify the Exchange vulnerability. It directs readers to a blog post that offers guidance on remediation for four ProxyLogon vulnerabilities.

The BlackCat ransomware family is gaining popularity thanks to its cross-platform capabilities that include functionality on Windows and Linux operating systems and VMWare instances. "It has extensive capabilities, including self-propagation configurable by an affiliate for their usage and to environment encountered," Microsoft says. That means no two deployments of its offering might look the same.
