



Published on *Inside Higher Ed*  
(<https://www.insidehighered.com>)

[Home](#) > FBI Warns of Increased Ransomware Attacks Targeting Colleges



## FBI Warns of Increased Ransomware Attacks Targeting Colleges

Submitted by Lindsay McKenzie on March 18, 2021 - 3:00am

A group of cybercriminals is increasingly targeting colleges, schools and seminaries and attempting to extort them, the FBI's Cyber Division has warned.

In an [advisory](#) <sup>[1]</sup> to cybersecurity professionals and system administrators published Tuesday, the FBI said that criminals are leveraging software called PYSAs ransomware to access IT networks, block access to vital information and systems through encryption, and demand payment to restore access.

In a [double-extortion tactic](#) <sup>[2]</sup> that has also been employed by criminals using other types of ransomware, the criminals are not only requesting payment in exchange for making encrypted data accessible again. They are also threatening to sell sensitive information such as Social Security numbers on the dark web if institutions or affected individuals do not meet demands.

PYSA ransomware, also known as Mespinoza, has recently been used in attacks on educational institutions in 12 U.S. states and the United Kingdom, the FBI reported. The agency became aware of PYSA in March 2020. In addition to educational institutions, the ransomware has been involved in attacks on government entities, private companies and the health-care sector. The criminals behind PYSA ransomware have not been identified.

The FBI said that the criminals often gain access to IT networks through phishing emails or stolen log-in credentials. Files ending in the .pysa extension are characteristic of a compromise, the agency said. It also provided a long list of email addresses associated with ransom demands.

To make it more difficult for criminals to gain access, the FBI advises that institutions use multifactor authentication, regularly patch software and systems, encourage users not to use public Wi-Fi networks, and train employees and staff members on ransomware and phishing scams.

"The FBI does not encourage paying ransoms," the advisory said. "Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."

The FBI encourages any institution to report suspected ransomware attacks or attempts to its local FBI field office or the FBI's [Internet Crime Complaint Center](#) <sup>[3]</sup>.

A list of domains the FBI said are associated with the ransom notes follows:

- ced\_cririele93@protonmail.com
- irvingalfie@protonmail.com
- gustaf.wixon@protonmail.com
- ralfgriffin@protonmail.com
- korgy.torky@protonmail.com
- astion11@protonmail.com
- Bfgkwethnsb@protonmail.com
- Logan\_A\_Gray@protonmail.com

- rafaeldari@onionmail.org
- Abelzackary@onionmail.org
- Elliotstaarss1@protonmail.com
- TimWestbrook@onionmail.org
- PaulDade@onionmail.org
- CarmenWashingtonGton@portonmail.com
- cozmo.storton@protonmail.com
- karim.abson@protonmail.com
- chettle.willem@protonmail.com
- dalliss.prout96@protonmail.com
- karreck.arch@protonmail.com
- keefe.mcmeckan@protonmail.com
- keepupchell@protonmail.com
- gabriel8970@protonmail.com
- masonhoyt@onionmail.org
- merry.lane@mailfence.com
- Jamesy.kettlewell@protonmail.com
- platt.lucais@protonmail.com
- jarret.wharram@protonmail.com
- hewitt\_rogers@protonmail.com
- thorvald\_beattie@protonmail.com
- warden\_riddoch@protonmail.com
- cowland\_lothaire@protonmail.com
- Nickola\_men@protonmail.com
- veronabello@onionmail.org
- giuliacabello@onionmail.org
- avitacabrera@protonmail.com
- domenikuvoker@protonmail.com
- mespinoza980@protonmail.com
- ellershaw.kiley@protonmail.com
- jonivaeng@protonmail.com
- alanson\_street8@protonmail.com
- raingemaximo@protonmail.com
- mcpherson.artair@protonmail.com
- lambchristoffer@protonmail.com
- gareth.mckie3l@protonmail.com
- rohrbacherlucho@protonmail.com
- aireyeric@protonmail.com
- noblecocking@protonmail.com
- presleybarry63@protonmail.com
- duncan\_cautherey@protonmail.com
- shdujdsh@protonmail.com
- ihdtwesfs@portonmail.com
- williamjohnson1963@protonmail.com
- casualstroons@portonmail.com
- izak.pollington@protonmail.com
- t\_trstram@protonmail.com
- willmottlem01@protonmail.com
- BettyRacine@protonmail.com
- Ohsgsuywb@protonmail.com
- Lojdgseywu@protonmail.com
- Johnbeamvv@protonmail.com
- rewhgsch@protonmail.com
- lhdbeydsdq@protonmail.com
- mario1@mailfence.com

---

**Source URL:** <https://www.insidehighered.com/quicktakes/2021/03/18/fbi-warns-increased-ransomware-attacks-targeting-colleges>

#### Links

[1] <https://www.ic3.gov/Media/News/2021/210316.pdf>

[2] <https://www.insidehighered.com/news/2020/06/11/colleges-face-evolving-cyber-extortion-threat>

[3] <https://ic3.gov/>