RansomBoggs: New ransomware targeting Ukraine

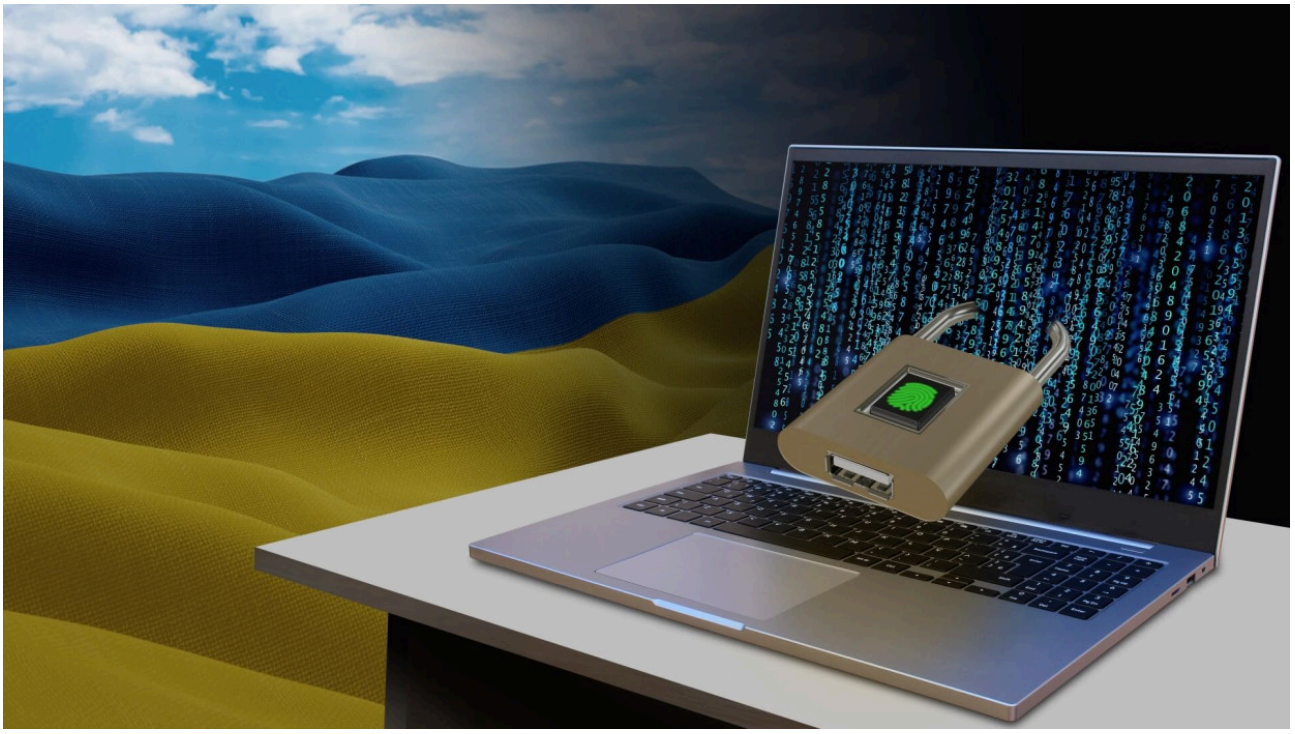
By Editor

Archived: 2026-04-05 22:53:43 UTC

Ukraine Crisis – Digital Security Resource Center

ESET researchers spot a new ransomware campaign that goes after Ukrainian organizations and has Sandworm's fingerprints all over it

28 Nov 2022 • , 2 min. read

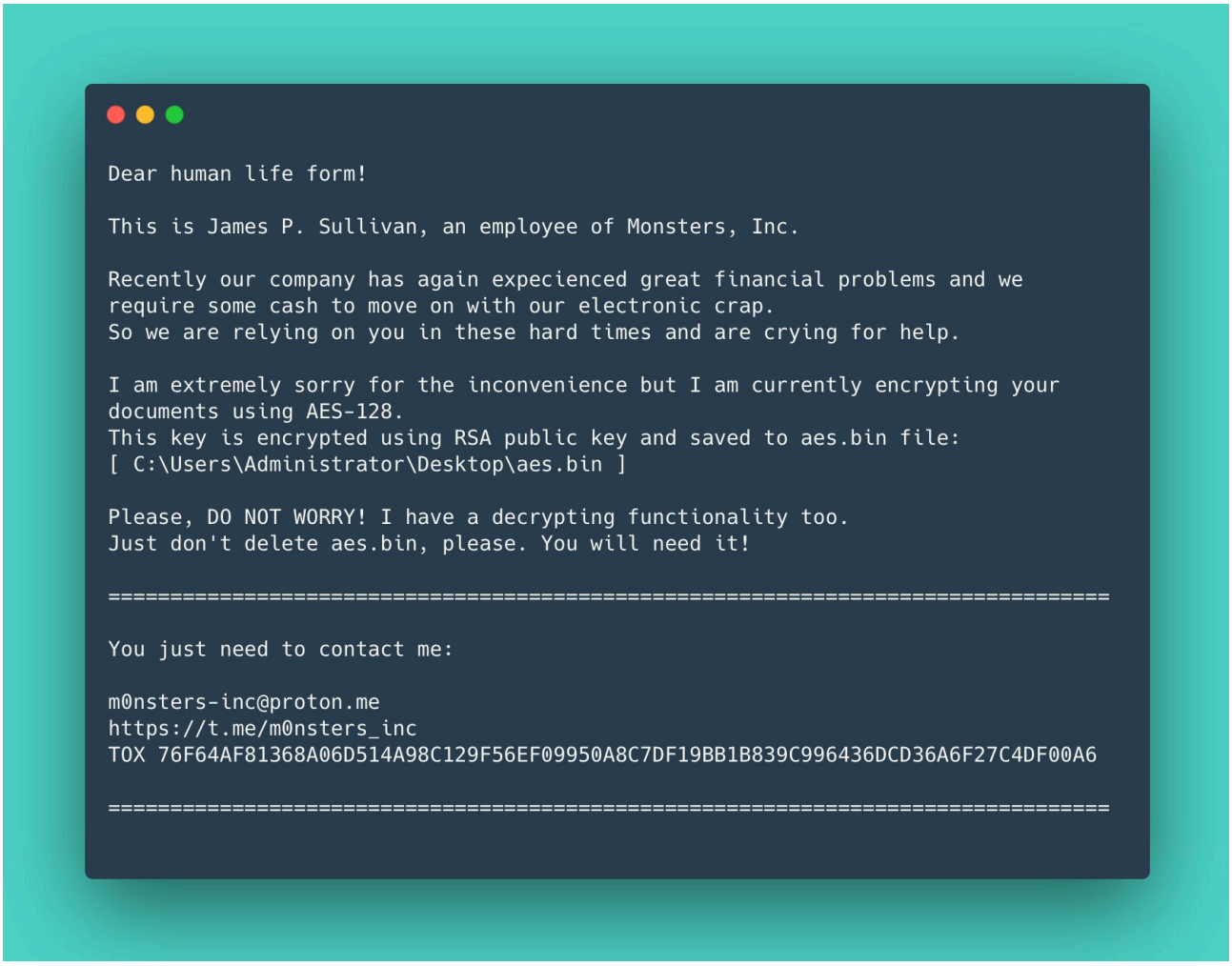


The ESET research team has spotted a new wave of ransomware attacks taking aim at multiple organizations in Ukraine and bearing the hallmarks of other campaigns previously unleashed by the Sandworm APT group.

Even though the ransomware – called RansomBoggs by ESET and written in the .NET framework – is new, particularly the way it is deployed bears close resemblance to some past attacks attributed to the notorious threat actor.

ESET has alerted Ukraine's Computer Emergency Response Team (CERT-UA) about the RansomBoggs onslaughts, which were first detected on November 21st. Depending on the variant, RansomBoggs is detected by ESET products as MSIL/Filecoder.Sullivan.A and MSIL/Filecoder.RansomBoggs.A.

RansomBoggs at a glance



RansomBoggs ransom note

In the ransom note seen above (SullivanDecryptsYourFiles.txt), the authors of RansomBoggs make multiple references to the Monsters Inc. movie, including by impersonating James P. Sullivan, the movie's main protagonist.

Once unleashed, the new ransomware "generates a random key and encrypts files using AES-256 in CBC mode" – not the AES key length of 128 bits mentioned in the ransom note. It then appends the .chsch extension to the encrypted files.

"The key is then RSA encrypted and written to aes.bin," said ESET researchers. Depending on the variant, the RSA public key is either hardcoded in the malware sample itself or provided as argument.

As for similarities with other onslaughts by Sandworm, the PowerShell script used to distribute RansomBoggs from the domain controller is almost identical to the one used in Industroyer2 attacks against Ukraine's energy sector in April of this year. The same script was used to deliver data-wiping malware called CaddyWiper that leveraged the ArguePatch loader and hit several dozen systems in a limited number of organizations in Ukraine in March.

Ukraine under fire

Sandworm has a long track record of being behind some of the world's most disruptive cyberattacks of the past near-decade. It last entered the spotlight just weeks ago after it was fingered by Microsoft as being behind ransomware called "Prestige" that hit several logistics companies in Ukraine and Poland in early October.

The aforementioned attacks do by no means give the full picture of the various threats that high-profile Ukrainian organizations have had to weather this year alone. For example, back on February 23rd, just hours before Russia invaded Ukraine, ESET telemetry picked up HermeticWiper on the networks of several Ukrainian organizations. The next day, a second destructive attack against a Ukrainian governmental network started, this time delivering IsaacWiper.

Indeed, Ukraine has been on the receiving end of a number of highly disruptive cyberattacks by Sandworm since at least 2014, including BlackEnergy, GreyEnergy and the first iteration of Industroyer. The group was also behind the NotPetya attack that swept through many corporate networks in Ukraine in June 2017 before spreading like wildfire globally and wreaking havoc in many organizations worldwide.

Further resources:
ESET Research webinar: How APT groups have turned Ukraine into a cyber-battlefield
ESET APT Activity Report T2 2022