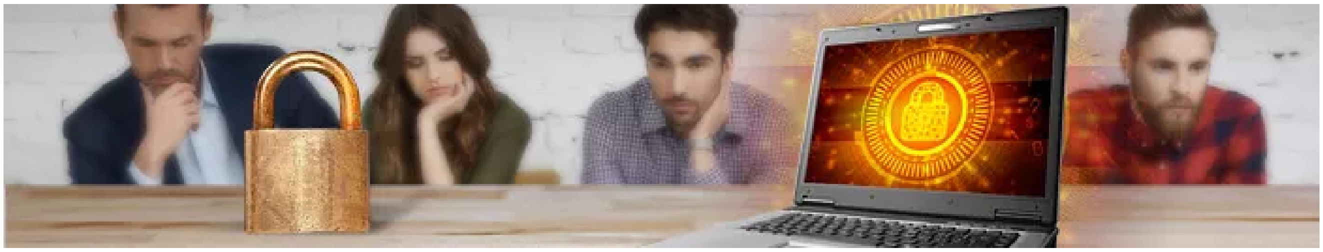
Apocalypse: Ransomware which targets companies through insecure RDP

blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

Sarah

June 29, 2016

Beyond a shadow of a doubt 2016 has been the year of the ransomware. So it comes as no surprise that new ransomware families are popping up on weekly basis. Emsisoft has been on the frontline battling ransomware for years now, providing users with valuable tools allowing them to recover their files after ransomware attacks. As a result Emsisoft researchers often find themselves at the receiving end of hate from ransomware authors. Late last year, we took a look at Radamant, whose authors included some rather unkind messages after our research team broke their amateurish ransomware. Today, we want to take a look at a new ransomware family Apocalypse, that reared its ugly head about 2 months ago, that recently started spewing insults towards our team as well.



Meet Apocalypse

The Apocalypse ransomware was first seen on the 9th May. The main attack vector is weak passwords on insecurely configured Windows servers running the remote desktop service. This allows an attacker to use brute force to gain access and means they can easily interact with the system as if they had access in person. Abusing remote desktop has become increasingly common over the last few months, especially for running ransomware like Apocalypse.

The earliest variants install themselves to %appdata%windowsupdate.exe and create a run key called *windows update* to both HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE. This variant uses the .encrypted extension. A ransom note is created for every file in the form of **filename*.How_To_Decrypt.txt*. The [email protected]/[email protected]/[email protected]/[email protected] email addresses are used in the ransom note.

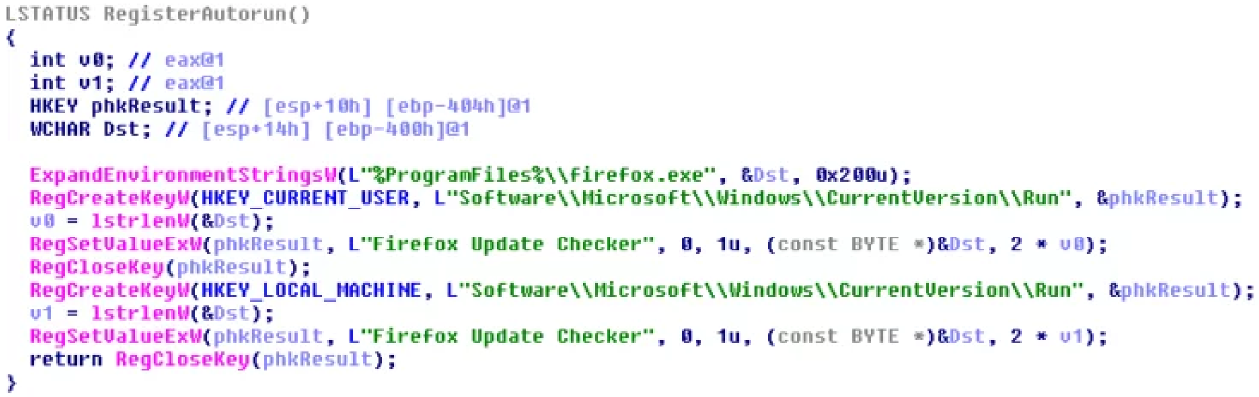
On June 9th, another version of the Apocalypse was discovered. This variant uses a different location, run key name and email address. The ransomware installs itself to %ProgramFiles%windowsupdate.exe, and creates a run key called *windows update svc*. The email address used in this variant is [email protected]

On June 22nd, the newest variant was discovered, which changed a lot more. Instead of using windowsupdate, it uses firefox as a name instead. The newest version installs itself to %ProgramFiles%firefox.exe, and creates a run key called *firefox update checker*. The new extension is .SecureCrypted and new name for ransom note **filename*.Contact_Here_To_Recover_Your_Files.txt*. The email address used is [email protected]

A closer look into the latest variant

To give you a better idea on how Apocalypse operates, we want to take a closer look at one of the newest variants with the hash AC70F2517698CA81BF161645413F168C. The ransomware first checks the default system language and if it is set to Russian, Ukrainian or Belarusian then the ransomware will quit and not encrypt the system.

The ransomware then copies itself to %ProgramFiles%firefox.exe, if it doesn’t exist there already, and sets the hidden and system attributes. It also falsifies the timestamp of this file using the explorer.exe timestamp. Then a run value is created, so the ransomware can run on every startup:



```
LSTATUS RegisterAutorun()
{
  int v0; // eax@1
  int v1; // eax@1
  HKEY phkResult; // [esp+10h] [ebp-404h]@1
  WCHAR Dst; // [esp+14h] [ebp-400h]@1

  ExpandEnvironmentStringsW(L"%ProgramFiles%\\firefox.exe", &Dst, 0x200u);
  RegCreateKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult);
  v0 = lstrlenW(&Dst);
  RegSetValueExW(phkResult, L"Firefox Update Checker", 0, 1u, (const BYTE *)&Dst, 2 * v0);
  RegCloseKey(phkResult);
  RegCreateKeyW(HKEY_LOCAL_MACHINE, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult);
  v1 = lstrlenW(&Dst);
  RegSetValueExW(phkResult, L"Firefox Update Checker", 0, 1u, (const BYTE *)&Dst, 2 * v1);
  return RegCloseKey(phkResult);
}
```

Creation of the run values

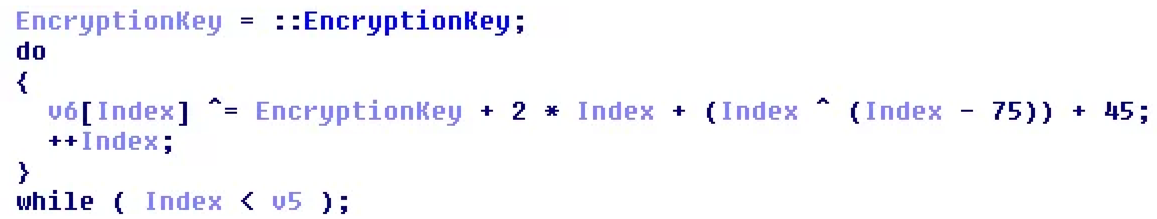
Once installation is complete, it then runs the newly created firefox.exe, which then deletes the file. The firefox.exe file does two different tasks at the same time: First, it periodically checks whether certain Windows processes are running and then kills them. Second, it starts the encryption routine where it gets a list of all removable, fixed or remote network drives; the latter however is never encrypted due to a bug in the ransomware. The ransomware then scans all folders and any files found will be encrypted.

However, the malware will not attempt to encrypt any files if they end in one of the following text strings:

- .exe
- .dll
- .sys
- .msi
- .com
- .lnk
- .tmp
- .ini
- .SecureCrypted
- .bin
- .bat
- .dat
- .Contact_Here_To_Recover_Your_Files.txt

Files located in the Windows folder are skipped as well.

To encrypt a file, the ransomware first checks whether it is encrypted already by comparing the first four bytes of the file against the magic value: 0xD03C2A77. If the file is not encrypted already then it will encrypt the content of the file in memory using a custom XOR based algorithm:



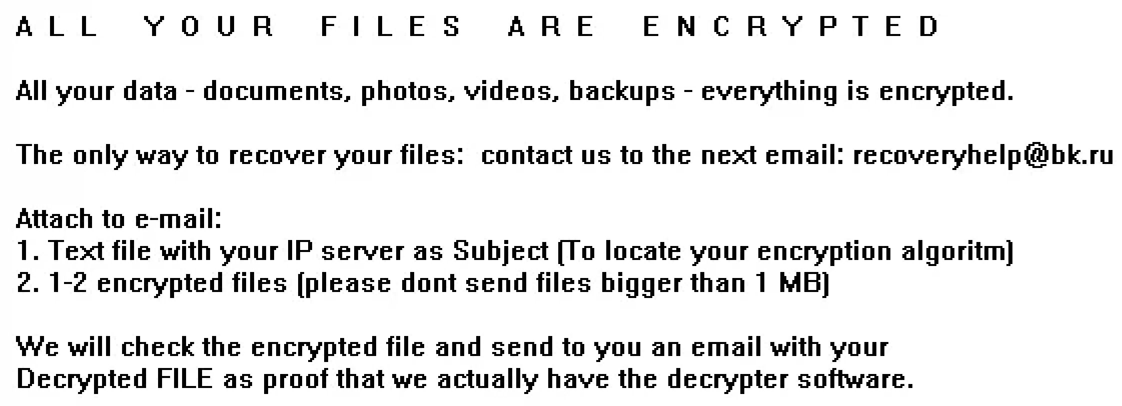
```
EncryptionKey = ::EncryptionKey;
do
{
  v6[Index] ^= EncryptionKey + 2 * Index + (Index ^ (Index - 75)) + 45;
  ++Index;
}
while ( Index < v5 );
```

Example of a Apocalypse encryption loop

The exact algorithm varies slightly from variant to variant. The magic value and encrypted content will then be written to the file and SecureCrypted is added to the filename. Before closing it, the original file timestamps will be restored and the following ransom note is created for the file:

> ALL YOUR FILES ARE ENCRYPTED
>
> All your data – documents, photos, videos, backups – everything is encrypted.
>
> The only way to recover your files: contact us to the next email: [email protected]
>
> Attach to e-mail:
> 1. Text file with your IP server as Subject (To locate your encryption algoritm)
> 2. 1-2 encrypted files (please dont send files bigger than 1 MB)
>
> We will check the encrypted file and send to you an email with your
> Decrypted FILE as proof that we actually have the decrypter software.
>
> Remember:
> 1. The FASTER you'll CONTACT US – the FASTER you will RECOVER your files.
> 2. We will ignore your e-mails without IP server number in Subject.
> 3. If you haven't received reply from us in 24 hours – try to contact us via public e-mail services such as Yahoo or so.

The ransomware also creates a window which it displays to the user with a similar ransom note:



ALL YOUR FILES ARE ENCRYPTED

All your data - documents, photos, videos, backups - everything is encrypted.

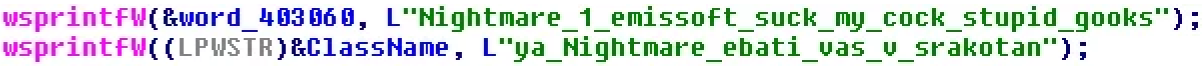
The only way to recover your files: contact us to the next email: recoveryhelp@bk.ru

Attach to e-mail:
1. Text file with your IP server as Subject (To locate your encryption algoritm)
2. 1-2 encrypted files (please dont send files bigger than 1 MB)

We will check the encrypted file and send to you an email with your
Decrypted FILE as proof that we actually have the decrypter software.

The screen that the ransomware displays to the user

One interesting aspect of this screen is that within the code which creates it, the ransomware author hid messages to Emsisoft:



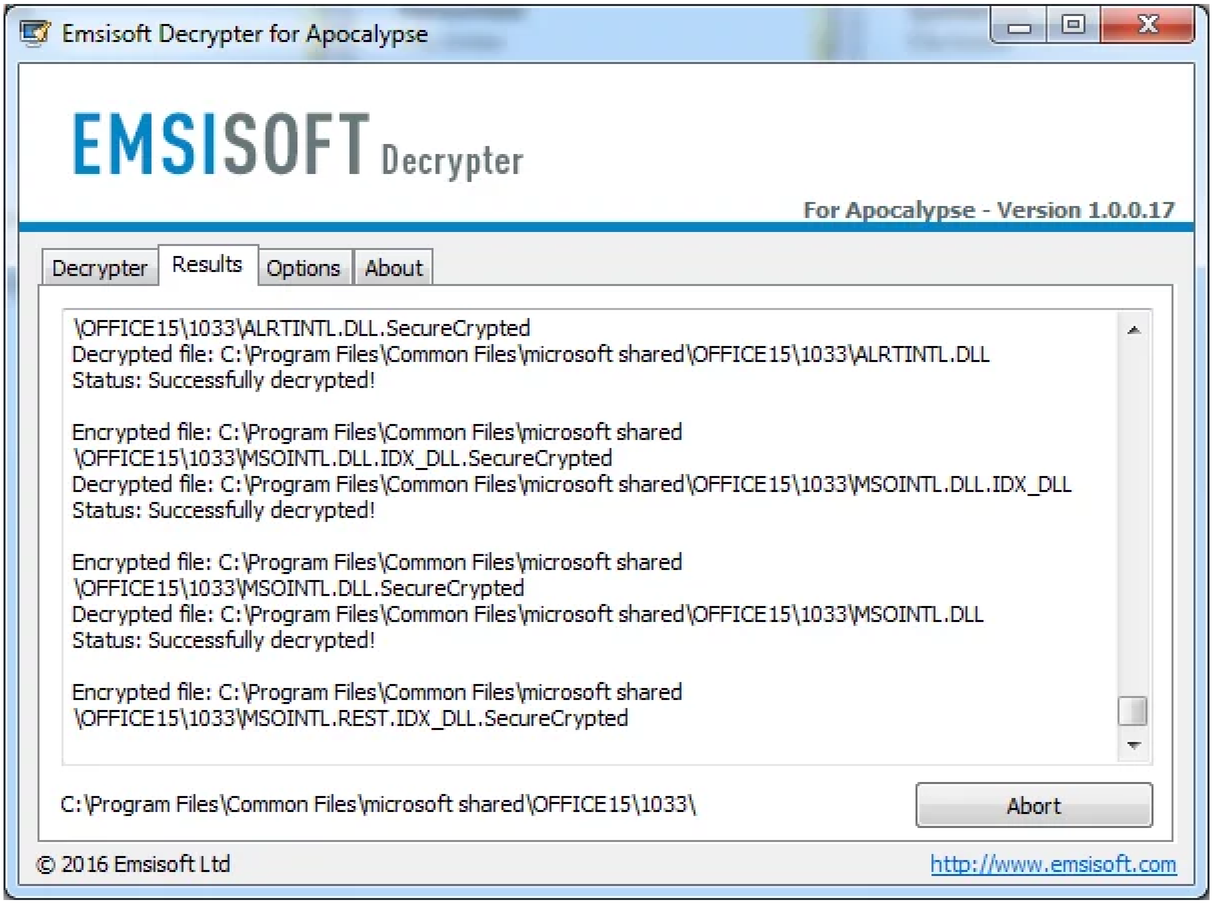
```
wsprintfW(&word_403060, L"Nightmare_1_emissoft_suck_my_cock_stupid_gooks");
wsprintfW((LPWSTR)&ClassName, L"ya_Nightmare_ebati_vas_v_srakotan");
```

The Apocalypse developer insults "emissoft"

As before, we see messages like this as validation of our work and consider it a backwards compliment.

How can I decrypt my files encrypted by this ransomware?

As for many other ransomware families, Emsisoft provides a free decrypter to all Apocalypse victims that allows them to decrypt their files for free.



```
\OFFICE15\1033\ALRTINTL.DLL.SecureCrypted
Decrypted file: C:\Program Files\Common Files\microsoft shared\OFFICE15\1033\ALRTINTL.DLL
Status: Successfully decrypted!

Encrypted file: C:\Program Files\Common Files\microsoft shared
\OFFICE15\1033\MSOINTL.DLL.IDX_DLL.SecureCrypted
Decrypted file: C:\Program Files\Common Files\microsoft shared\OFFICE15\1033\MSOINTL.DLL.IDX_DLL
Status: Successfully decrypted!

Encrypted file: C:\Program Files\Common Files\microsoft shared
\OFFICE15\1033\MSOINTL.DLL.SecureCrypted
Decrypted file: C:\Program Files\Common Files\microsoft shared\OFFICE15\1033\MSOINTL.DLL
Status: Successfully decrypted!

Encrypted file: C:\Program Files\Common Files\microsoft shared
\OFFICE15\1033\MSOINTL.REST.IDX_DLL.SecureCrypted
```

C:\Program Files\Common Files\microsoft shared\OFFICE15\1033\

The Emsisoft Apocalypse decrypter at work

The decrypter is available for download at our Emsisoft Decrypter portal here.

How can I protect myself?

Due to the nature of the attack protection software is rather ineffective. If the attacker manages to get access to the system via remote control, they can simply disable any protection software installed or add the malware to the protection software's exclusion list. It therefore is imperative to prevent the attacker from gaining access to the system to begin with.

The most important line of defense is a proper password policy that is enforced for all user accounts with remote access to the system. This does apply to rarely used accounts created for testing purposes or by applications as well.

Even better would be to disable Remote Desktop or Terminal Services completely if not required or at least to use IP address based restrictions to allow the access to these services from trusted networks only.