Spora - the Shortcut Worm that is also a Ransomware

gdatasoftware.com/blog/2017/01/29442-spora-worm-and-ransomware

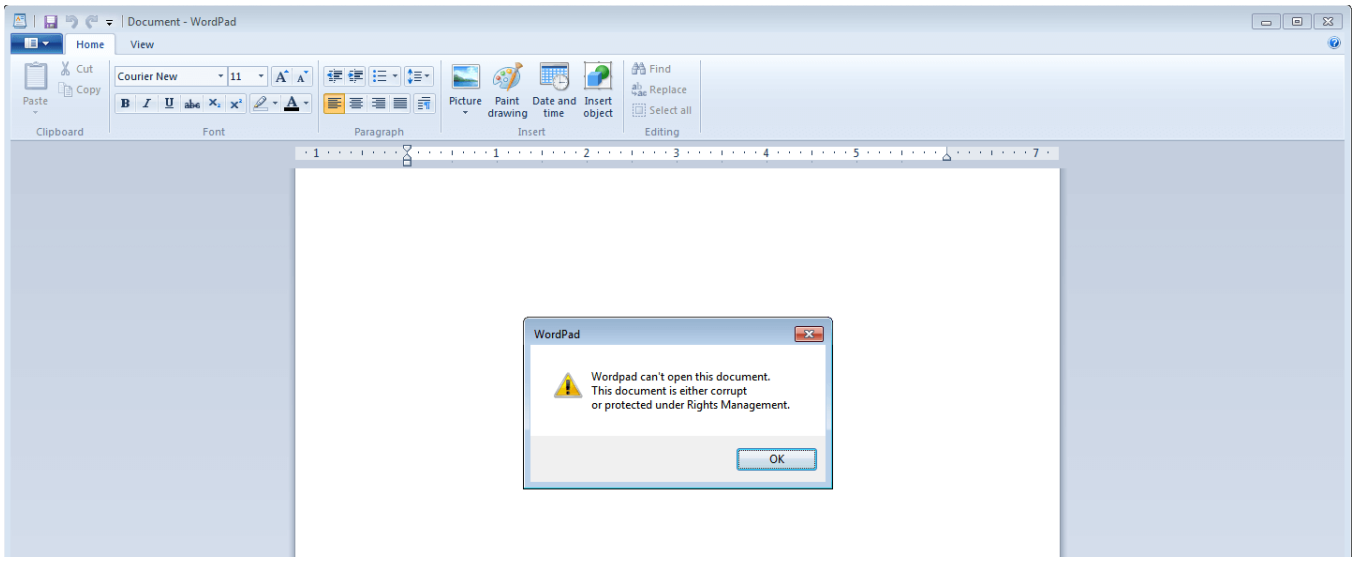
Spora spreads via USB drives like Gamarue and Dinihou aka Jenxcus whilst also encrypting files. The sophistication of this threat could easily make it the new Locky. We discuss its infection and encryption procedure and show how it uses statistical values about encrypted files to calculate the ransom amount.

HTA email Attachment as common infection vector

Spora's ransom note was first spotted by the ID Ransomware maintainers and announced via Twitter by MalwareHunterTeam. Several malware researchers and Twitter users were amazed by the good-looking, professional ransomware website and ransom note. Experience showed that most of these websites are in a bad shape. The first sample was provided by a member of Bleepingcomputer and discussed in their Spora support topic.

This sample is an HTA application with obfuscated VBScript code. According to Bleepingcomputer it arrived in a ZIP archive via email attachment. Submissions on VirusTotal show the filename Скан-копия _ 10 января 2017г. Составлено и подписано главным бухгалтером. Экспорт из 1С.a01e743_pdf.hta.

The HTA file writes a JScript file to %TEMP%\close.js and executes it. The JScript file in turn is a dropper for a Word document that is written to %TEMP%\doc_6d518e.docx and a PE file that is saved to %TEMP%\81063163ded.exe. Both files are opened by close.js, the Word document with a parameter to show and focus the window, and the PE file with a parameter to hide it. As a result the document will be opened by the set default application for .docx files, e.g., Word, but an error message is shown because it is corrupt. The PE file 81063163ded.exe has a seemingly random name, but it is actually hardcoded by the dropper. The PE file is UPX packed and contains the actual payload.



Error message, appears after opening the corrupt document

Worm-like behavior similar to Dinihou and Gamarue

While ZCryptor had already been deemed a combination of ransomware and worm due to its usage of autorun.inf, Spora goes some steps further using the same techniques as Gamarue and Dinihou. The functionality of autorun.inf had been removed in Windows 7 and was patched on Windows XP and Windows Vista more than seven years ago, thus making it an ineffective technique for worms to spread via removable drives. The trick is: Gamarue, Dinihou and now also Spora use Windows shortcuts (.LNK files) instead.

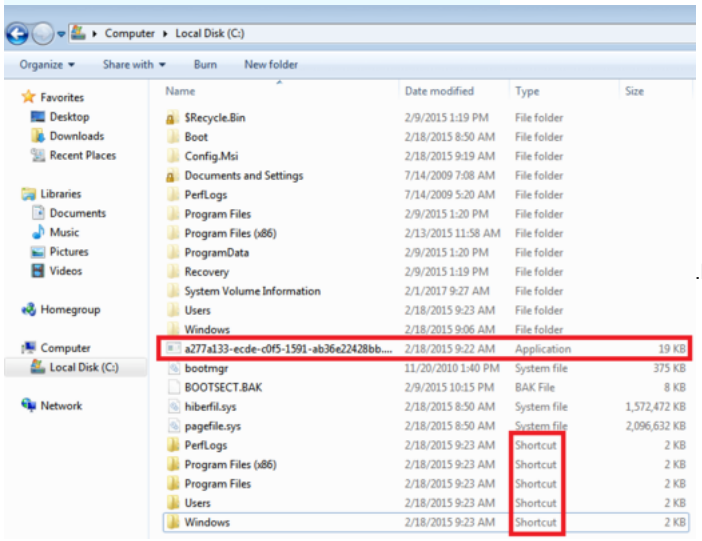
Spora adds the hidden attribute to files and folders on the desktop, in the root of removable drives and the system drive. These hidden files and folders are, with the standard folder options, not visible anymore. Spora then puts Windows shortcuts with the same name and icon as the hidden files and folders as a visible replacement. Those .LNK files open the original file to avoid raising any suspicion and simultaneously execute the malware. An example: the folder C:\Windows will be hidden and a file named C:\Windows.lnk will be created; it looks exactly like the original folder if the standard folder options on Windows are set.

The .LNK files use the following command to execute the worm and open the original file. If the original file is a folder it will open Windows Explorer to show its contents:

/c explorer.exe "<originalfile>" & type "<worm>" > "%%tmp%%\<worm>" & start "<originalfile>" "%%tmp%%\<worm>"

The worm copies itself as hidden file alongside the .LNK files, its filename is generated by calculating the CRC32 checksum for the VolumeSerialNumber. The result is put into the pattern %08x-%04x-%04x-%02x%02x-%02x%02x%02x%02 (see address 0x405492). This means, the name for the malware file can be, e.g., a277a133-ecde-c0f5-1591-ab36e22428bb.exe.

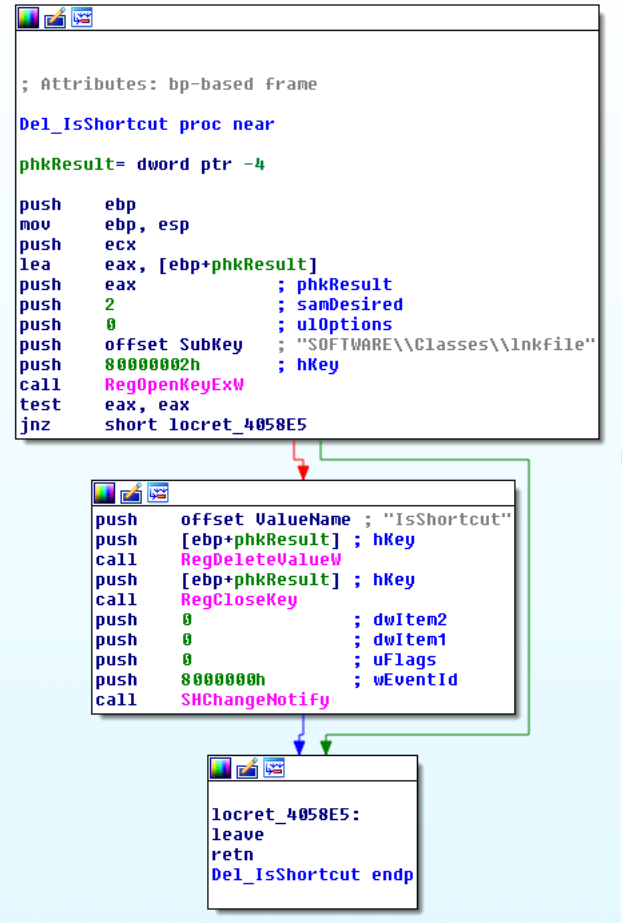
This function calculates the CRC32 based on the VolumeSerialNumber of the disk



.LNK files and a copy of the malware have been created in the root of the system drive.

The worm deletes the registry value HKCR\lnkfile\isShortcut with the effect that the shortcut icons don't show the characteristic bent arrow in the lower left corner, which would be telltale sign to the user that something is wrong.

Simply navigating through the folders on your system and desktop using double-click will execute the worm. Using this strategy, it will not only spread to removable drives like USB thumb drives, it will also encrypt newly created files on the system. This renders the system unusable, for storing or working on any pictures or documents, until it is disinfected.

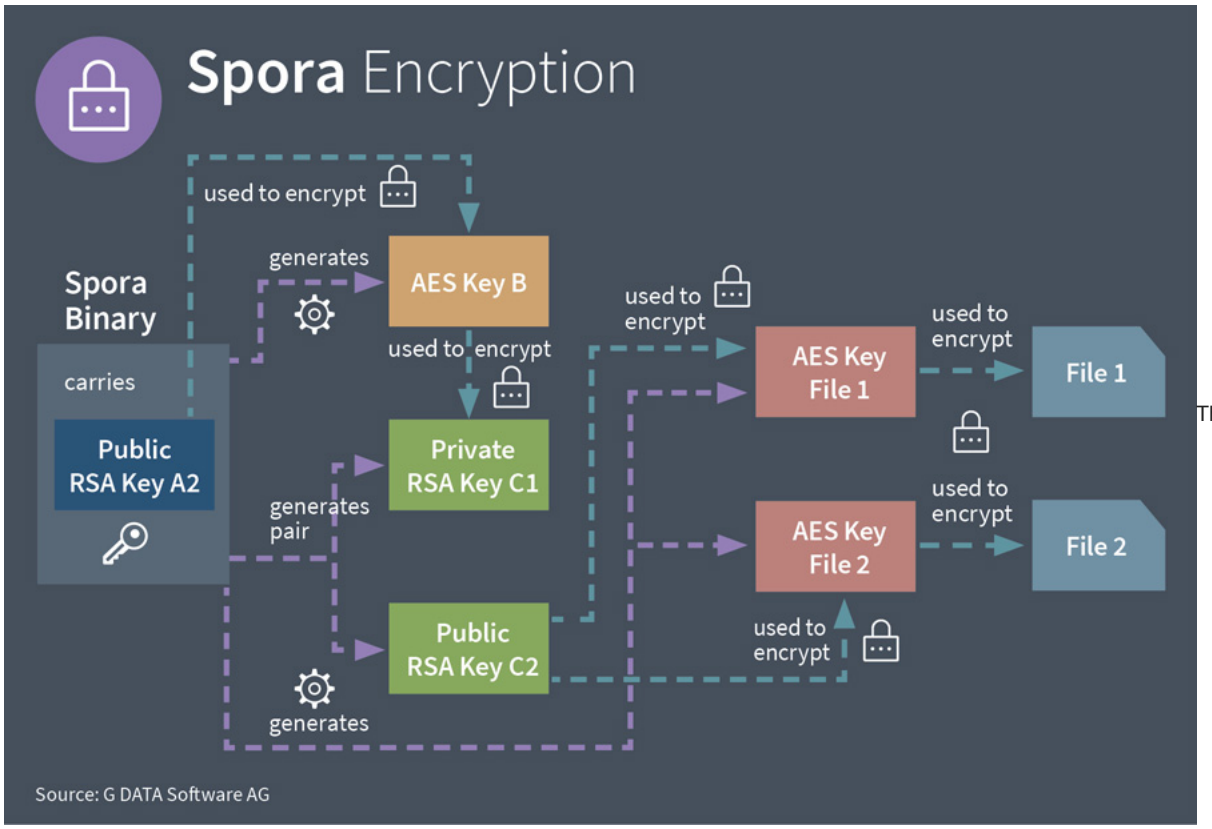


Function that deletes the isShortcut value in the registry

Encryption

Spora actually does not rename encrypted files and targets a comparably small set of extensions. The encryption procedure is shown in the diagram below.

.backup, .7z, .rar, .zip, .tiff, .jpeg, .jpg, .accdb, .sqlite, .dbf, .1cd, .mdb, .cd, .cdr, .dwg, .psd, .pdf, .odt, .rtf, .docx, .xlsx, .doc, .xls



The Spora encryption shown in an info graphic

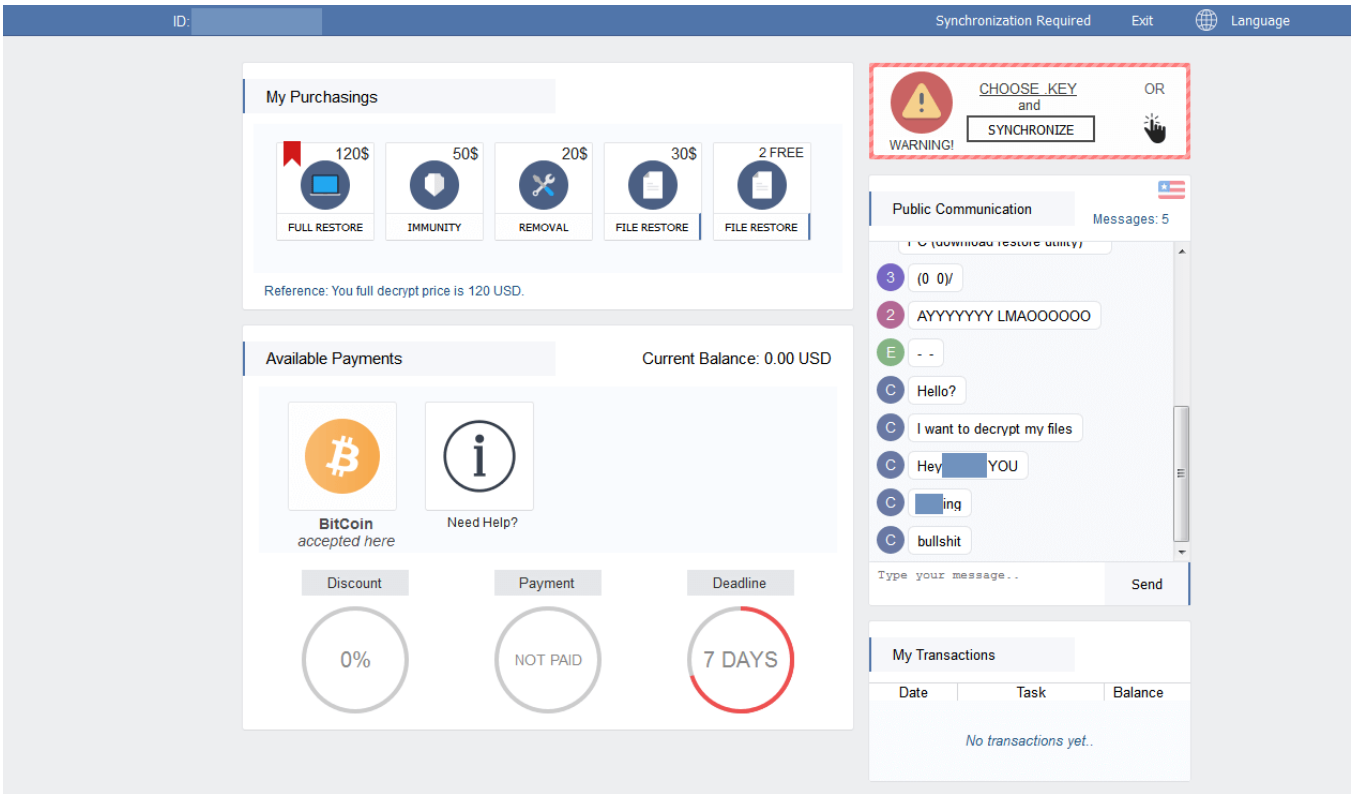
Spora generates a pair of RSA keys, C1 and C2 (1024 bit). This newly generated public RSA key C2 is used to encrypt the per-file AES keys which are also generated by Spora. The generated private RSA key C1 on the other hand is stored in the .KEY file. That file is encrypted using a newly generated AES Key B (256 bit). The attacker's public RSA key A2 is used to encrypt AES key B. The encrypted key B is appended to the .KEY file. The figure below shows the code that writes the .KEY file's content including the encrypted AES key B to disk.

A second important file is the .LST file which contains a list of all encrypted files. Its encryption works analogous to the .KEY file encryption. A new AES key is generated, used to encrypt the .LST contents, encrypted by the public RSA key A2 of the attacker and appended to the .LST file in encrypted form (see screenshot below):

The encrypted content of the .KEY file and the encrypted AES Key are written to disk

AES key F is encrypted by public RSA key A and the .LST file contents are encrypted using AES key F (256 bit).
Using this encryption scheme, Spora does not have to obtain a key from a command and control server and can work offline. The user has to upload the .KEY file to the payment site.

The .KEY file is only decryptable by the ransomware authors. Using their private RSA key A1 they could decrypt the AES Key B that was appended to the .KEY file. They could decrypt the remaining .KEY file contents including the user's private RSA key C1 using AES key B. Then they may put the private RSA key C1 into a decrypter that they send to the user after they have received the payment. This handling ensures that the attackers' private RSA key A1 is not exposed and that the decrypter only works for one user.However, this also means that there is only one private RSA key A1 for several infections. If that key is leaked or obtained by law enforcement, it can be used to decrypt all files that were encrypted by this variant of Spora and as such we can consider it a master key.



The Spora payment site includes a chat system and provides several decryption packages with varying prices

Statistics about encrypted files

Spora counts the number of encrypted files for six different extension categories. They are listed in the table below.

Position/ID	Category	File Extensions
1	Office Document	.odt, .rtf, .docx, .xlsx, .doc, .xls

2	PDF	.pdf
3	CorelDraw, AutoCAD, Photoshop	.cdr, .dwg, .psd
4	Database	.accdb, .sqlite, .dbf, .1cd, .mdb, .cd
5	Image	.tiff, .jpeg, .jpg
6	Archive	.backup, .7z, .rar, .zip

The .KEY file saves these statistical values in the form date|user name|locale|cat1|cat2|cat3|cat4|cat5|cat6, e.g. 13.1.2017|horst|USA|10|2|3|0|103|51

The same statistics will be used for the naming scheme of the .LST file, the .KEY file and the ransom note. Let's take the following triplet of .KEY file, .LST file and ransom note as example.

- RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.LST
- RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.KEY
- RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.HTML

The first two letters of the filename are the locale which is RU in our example. The following five letters are the first characters of the MD5 hash for the contents of the .KEY file, in our example '30215'. The counters start right after the MD5 substring at the 8th letter. They have to be decoded using the substitution table below:

	1	2	3	4	5	6	7	8	9	I	Padding
Z	X	R	O	A	H	F	G	E	K	T	Y

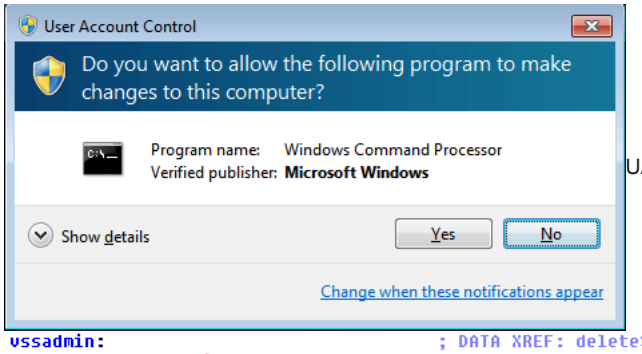
That means the file name RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY translates to Russia as location, the characters '30215' for the beginning of the MD5 hash, 12971 encrypted office documents, 6370 encrypted PDF, 8 encrypted CorelDraw/AutoCAD/Photoshop files, 9 encrypted database files, 16632 encrypted images and 144 encrypted archives.

After uploading the .KEY file to Spora's payment website, the ransom amount will be calculated depending on the number of encrypted files. The table below shows some examples, sorted by the amount of ransom asked (thanks to xXToffeeXx for providing these):

Office Documents	PDF	CorelDraw/AutoCAD/Photoshop	Databases	Images	Archives	Ransom in USD
2284	1550			1211	89	79 up to 110
489	471		4	796	6	79 up to 110
5223	374	206	12	12694	198	90 up to 120
7791	7341		2194	8587	782	128 up to 170
11160	9354	24	69	9774	242	146 up to 190
12851	5188	1851	51	331031	1281	199 up to 250
21173	7087	5	149	7069	730	214 up to 270
25146	25829	29598	5463	105943	5818	280 up to 350
138964	95087	218249	846	277541	22449	280 up to 350
11810	7272	15306	10	27651	1471	280 up to 350
30503	2135	40098	37	25271	1580	280 up to 350
26375	20505	12178	3016	31505	2487	280 up to 350
82319	40707	16931	114	38520	3607	280 up to 360

Additional behavior

Spora does not bypass User Account Control (UAC). This means, the user will be asked whether the malware is allowed to make changes to the computer in use. Spora deletes shadow volume copies and disables Windows error recovery and startup repair.



UAC asks for permission

```
vssadmin:                               ; DATA XREF: deleteShadows+28↓o
                unicode 0, <process call create "cmd.exe /c vssadmin.exe delete shado>
                unicode 0, <ws /all /quiet & bcdedit.exe /set {default} recoveryenabl>
                unicode 0, <ed no & bcdedit.exe /set {default} bootstatuspolicy ignor>
                unicode 0, <eallfailures">,0
                align 4
```

Shadow volume copy deletion

List of files involved

Filenames	Description	SHA256	Detected As
Скан-копия _ 10 января 2017г. Составлено и подписано главным бухгалтером. Экспорт из 1С.a01e743_pdf.hta	HTA dropper	3fb2e50764dea9266ca8c20681a0e0bf60feaa34a52699cf2cf0c07d96a22553	Script.Trojan-Dropper.Spora.A
close.js	JScript dropper	e2fe74d890ddb516b4f21a6588c6e0bdbf3dd6f8c5116d707d08db7ebddf505a	Script.Trojan-Dropper.Spora.G
81063163ded.exe, a277a133-ecde-c0f5-1591-ab36e22428bb.exe	Spora PE file, UPX packed	dbfd24cd70f02ddea6de0a851c1ef0f45f18b4f70e6f3d0f2e2aec0d1b4a2cbf	Win32.Worm.Spora.B
doc_6d518e.docx	Corrupt Word document	0ba39054a70802d0b59a18b873aab519e418dc9b0c81400d27614c9c085409ad	-
Windows.lnk	Malicious shortcut		Win32.Worm.SporaLnk.A
RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.HTML	Ransom note		-
RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.KEY	Contains statistics, campaignID, username, locale, timestamp and private RSA key C1; encrypted		-
RU302-15XRK-GXTFO-GZTET-KTXFF-ORTXA-AYYYY.LST	List of encrypted files; encrypted		-

- Malware
- Mails
- Microsoft Windows