## , Syskey!

© 2017 Passcape Software Passcape Software

1.			3
2.	Syske	<sub>2</sub> y	3
2.1	Syskey		3
2.2	syskey.exe		3
2.3		Syskey	4
2.3.1			4
2.3.2			4
2.3.3			
2.4	sy	skey.exe	5
3.	syskey.exe		5
3.1			5
3.2			5
3.3			6
3.4			6
4.			7
5.	1.		SAM
	Syskey		7
6.	2.	Syskey	8

	Windows 10 Fall Cr	eators Update	Windows Serve	er 2016 RS3	Microsoft
•		syskey.exe. Microsoft			
•			Syskey		
	,	,	Syskey ?	Syskey, ,	,
2 2.1	Syskey	skey			
	,	,			y. <b>Syskey</b> SAM
2.2	syskey.exe				
ľ	Syskey		,	Windows N V	T 4.0 SP3 Vindows XP
	,	Syskey,	syskey	? . Syskey. exe.	Microsoft

	Syskey					
	128-	Syskey	Syskey.	syskey.exe	:	
•						
		Syskey				
HKEY_LC	DCAL_MACH DCAL_MACH	INE\System INE\System	n\CurrentContr n\CurrentContr	rolSet\Control\Lsa\JD rolSet\Control\Lsa\Skew1 rolSet\Control\Lsa\Data rolSet\Control\Lsa\GBG		
		\$	, Syskey.			
	sysk	ey.exe		,		
			,	128-		
	,	Syskey		,		
,	,		·	, Windows		

2.4 syskey.exe

3 syskey.exe

syskey.exe, Microsoft.

3.1

```
Syskey

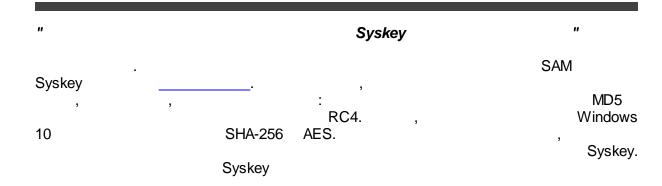
skype/IE/chrome/wifi/lan

Syskey

Windows
Syskey

Syskey
```

3.2



```
10-20
                                                                               100.
                   ).
                                       Syskey
                                                                              100
                                         Windows.
                                                                   Syskey
                                                                                      'Letmein123'
3.3
                                                         Misrosoft.
                                                      EFS.
                                  Microsoft
                                                                       Bitlocker.
                                                     Bitlocker
                                                                                  Microsoft,
                                                                        Microsoft.
                                                    Active Directory,
                                Bitlocker
3.4
          2014-2017
                                          Windows
                                                     syskey.exe.
        Microsoft.
                                                  John Smith,
                                                              syskey.exe
                            Syskey.
        syskey-
                                                                                     Syskey.
                                   syskey.exe
                                                                Microsoft,
                                Syskey,
                                             Syskey.
```

## net user USERNAME NEWPASSWORD

```
4
                                               Windows 10 Fall Creators Update
                syskey.exe,
                                            Microsoft
              Microsoft.
5
                         Syskey
       SAM
       BYTE hash[16], pDecodedData[32];
       static BYTE samc1[]="!@#$%/&*()qwertyUIOPAzxcvbnmQQQQQQQQQQQQ()(*@&%";
       static BYTE samc2[]="01234567890123456789012345678901;
       //Generate decrypt key
       Md5Init();
       Md5Update(pSamSessionKey+8,16);
       Md5Update(samc1,0x2F);
       Md5Update(m_pSyskey,16);
       Md5Update(samc2,0x29);
       Md5Final(hash);
       //Decrypt
       memcpy(pDecodedData,pSamSessionKey+24,32);
       Rc4SetKey(hash,16);
       Rc4Decrypt(pDecodedData,32);
       //Check sign
       Md5Init();
       Md5Update(pDecodedData,16);
       Md5Update(samc2,0x29);
       Md5Update(pDecodedData,16);
       Md5Update(samc1,0x2F);
       Md5Final(hash);
```

```
if( memcmp(pDecodedData+16,hash,16)==0 )
          memcpy(pDecodedSamSessionKey,pDecodedData,16);
          return TRUE;
       return FALSE;
                        2.
6
                                             Syskey
       BOOL DecryptSyskey(LPCTSTR szJD, LPCTSTR szSkew1, LPCTSTR szGBG, LPCTSTR szData)
          BYTE p[]=\{0xb,0x6,0x7,0x1,0x8,0xa,0xe,0x0,0x3,0x5,0x2,0xf,0xd,0x9,0xc,0x4\};
          BYTE pEncryptedKey[16];
          if(!szJD ||!szSkew1 ||!szGBG ||!szData)
            return FALSE;
         //convert to binary
          _stscanf_s(szJD,_T("%X"),(LPDWORD)&pEncryptedKey[0]);
         _stscanf_s(szSkew1,_T("%X"),(LPDWORD)&pEncryptedKey[4]);
          _stscanf_s(szGBG,_T("%X"),(LPDWORD)&pEncryptedKey[8]);
         _stscanf_s(szData,_T("%X"),(LPDWORD)&pEncryptedKey[12]);
          //Permutate
          for( int i=0; i<16; i++)
            m_pSyskey[i]=pEncryptedKey[p[i]];
          return TRUE;
       }
```