GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension

bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension

By
Lawrence Abrams

- January 29, 2018
- 09:21 PM
- 2

A new ransomware called GandCrab was released towards the end of last week that is currently being distributed via exploit kits. GandCrab has some interesting features not seen before in a ransomware, such as being the first to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld.

First discovered by security researcher David Montenegro, researchers quickly jumped in to analyze the ransomware and post their results on Twitter. This article will dive into what has been discovered by myself and other researchers.

Unfortunately, at this time there is no way to decrypt files encrypted by GandCrab for free. This ransomware is being researched, though, and if any new information is released we will be sure to update this article.

For now, if you wish to discuss GandCrab you can this article's comments section or our dedicated GandCrab Help & Support Topic.

GandCrab being distributed through the Rig exploit kit

According to exploit kit researchers nao_sec and Brad Duncan, GandCrab is currently being distributed through a malvertising campaign called Seamless that then pushes the visitors to the RIG exploit kit. The exploit kit will then attempt to utilize vulnerabilities in the visitor's software to install GandCrab without their permission.

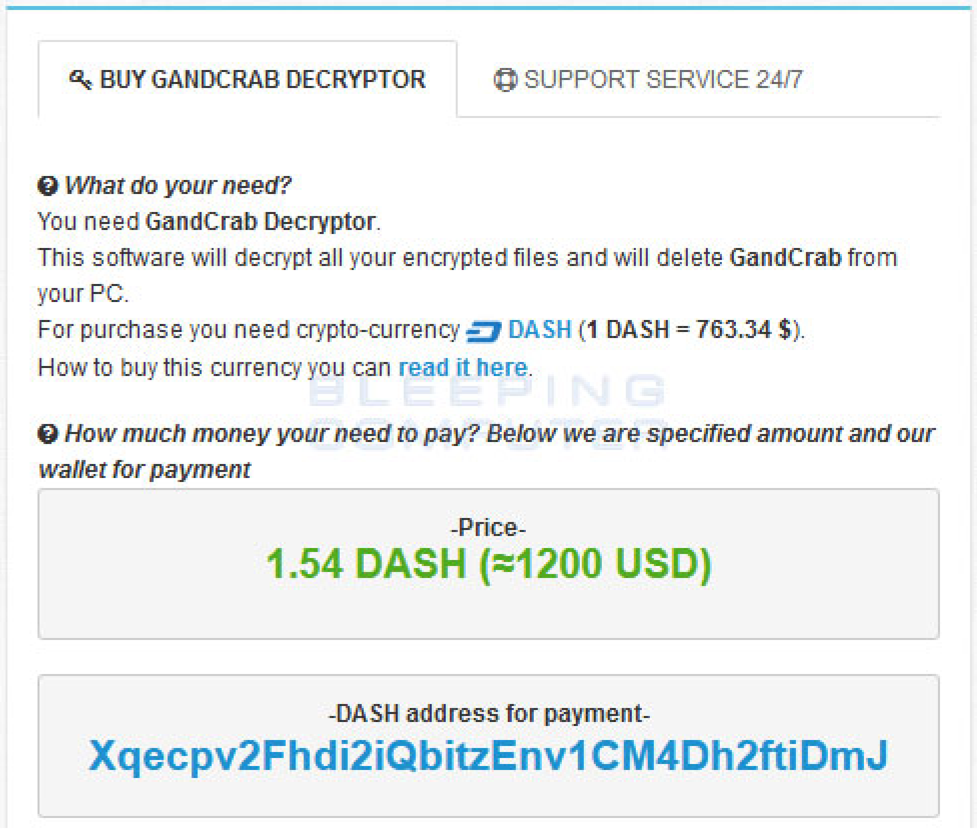
> Hi @anyrun_app, you're agile! I found #GandCrab, from #Seamless campaign (only gate4)🤔
> https://t.co/bt0GgJsfbF
> CC: @VK_Intel @James_inthe_box @malware_traffic
>
> — nao_sec (@nao_sec) January 26, 2018

If the exploit kit is able to install the ransomware, the victim will probably not realize they are infected until it is too late.

GandCrab is the first ransomware to use the Dash Currency

A first for ransomware is GandCrab's use of the DASH currency as a ransom payment. Most file encrypting ransomware families have exclusively used Bitcoin as the ransom payment method. Lately, some ransomware infections have been moving to Monero and even Ethereum.

This is the first time, though, that we have seen any ransomware ask for DASH as the payment. This is most likely due to DASH being built around privacy and thus harder for law enforcement to track the owners of the coins.



BUY GANDCRAB DECRYPTOR

SUPPORT SERVICE 24/7

What do your need?

You need **GandCrab Decryptor**.

This software will decrypt all your encrypted files and will delete **GandCrab** from your PC.

For purchase you need crypto-currency DASH (**1 DASH** = **763.34 $**).

How to buy this currency you can read it here.

How much money your need to pay? Below we are specified amount and our wallet for payment

-Price-

1.54 DASH (≈1200 USD)

-DASH address for payment-

Xqecpv2Fhdi2iQbitzEnv1CM4Dh2ftiDmJ

DASH Current as Payment

The GandCrab developers are currently asking for 1.54 DASH, which is approximately $1,170 USD at today's prices.

GandCrab utilizes NameCoin's .BIT TLD

Another interesting feature is GandCrab's use of the NameCoin .BIT top-level domain. .BIT is not a TLD that is recognized by the Internet Corporation for Assigned Names and Numbers (ICANN), but is instead managed by NameCoin's decentralized domain name system.

This means that any software that wishes to resolve a domain name that uses the .BIT tld, must use a DNS server that supports it. GandCrab does this by making dns queries using the a.dnspod.com DNS server, which is accessible on the Internet and can also be used to resolve .bit domains.

GandCrab uses these .bit domains as addresses for its Command & Control servers. Interestingly, the domain servers used by this ransomware contain names that you might recognize.

```
bleepingcomputer.bit
nomoreransom.bit
esetnod32.bit
emsisoft.bit
gandcrab.bit
```

After the publication of this story, the NameCoin developers issued a statement explaining that even though the GandCrab devs tried to use NameCoin DNS for their command & control servers, they did not set it up correctly. Instead the NameCoin developers stated that dnspod.com was just allowing the use of .bit domains even though it is not a TLD recognized by ICANN.

How GandCrab encrypts a computer

When GandCrab is first launched it. will attempt to connect to the ransomware's Command & Control server. As this server is hosted on one of Namecoin's .bit domains, it has to query a name server that supports this TLD.

It does this by querying for the addresses of the following domains using the command **nslookup [insert domain] a.dnspod.com**. This command queries the a.dnspod.com name server, which support the .bit TLD, for one of the domains below.

```
bleepingcomputer.bit
nomoreransom.bit
esetnod32.bit
emsisoft.bit
gandcrab.bit
```

If the victim's machine is unable to connect to the C2 server, then the ransomware will not encrypt the computer. It will, though, continue running in the background trying to get the IP address for the C2 and connect to it.

Once it is able to resolve the domain, it will connect to the C2 server's IP address. It is not known at this time what data is being sent and retrieved, but the C2 is most likely sending the public key that should be used to encrypt the files.

During this process, the ransomware will also connect to http://ipv4bot.whatismyipaddress.com/ to determine the public IP address of the victim.

Before GandCrab encrypts the victim's files it will first check for certain processes and terminate them. This will close any file handles that are open by these processes so that they can be properly encrypted. According to security researcher Vitali Kremez, the list of processes that are terminated are:

```
msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe,
ocssd.exe, dbsnmp.exe, synctime.exe, mydesktopqos.exe, agntsvc.exeisqlplussvc.exe,
xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, agntsvc.exeagntsvc.exe,
agntsvc.exeencsvc.exe, firefoxconfig.exe, tbirdconfig.exe, ocomm.exe, mysqld.exe,
mysqld-nt.exe, mysqld-opt.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe,
infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe,
steam.exe, thebat.exe, thebat64.exe, thunderbird.exe, visio.exe, winword.exe,
wordpad.exe
```

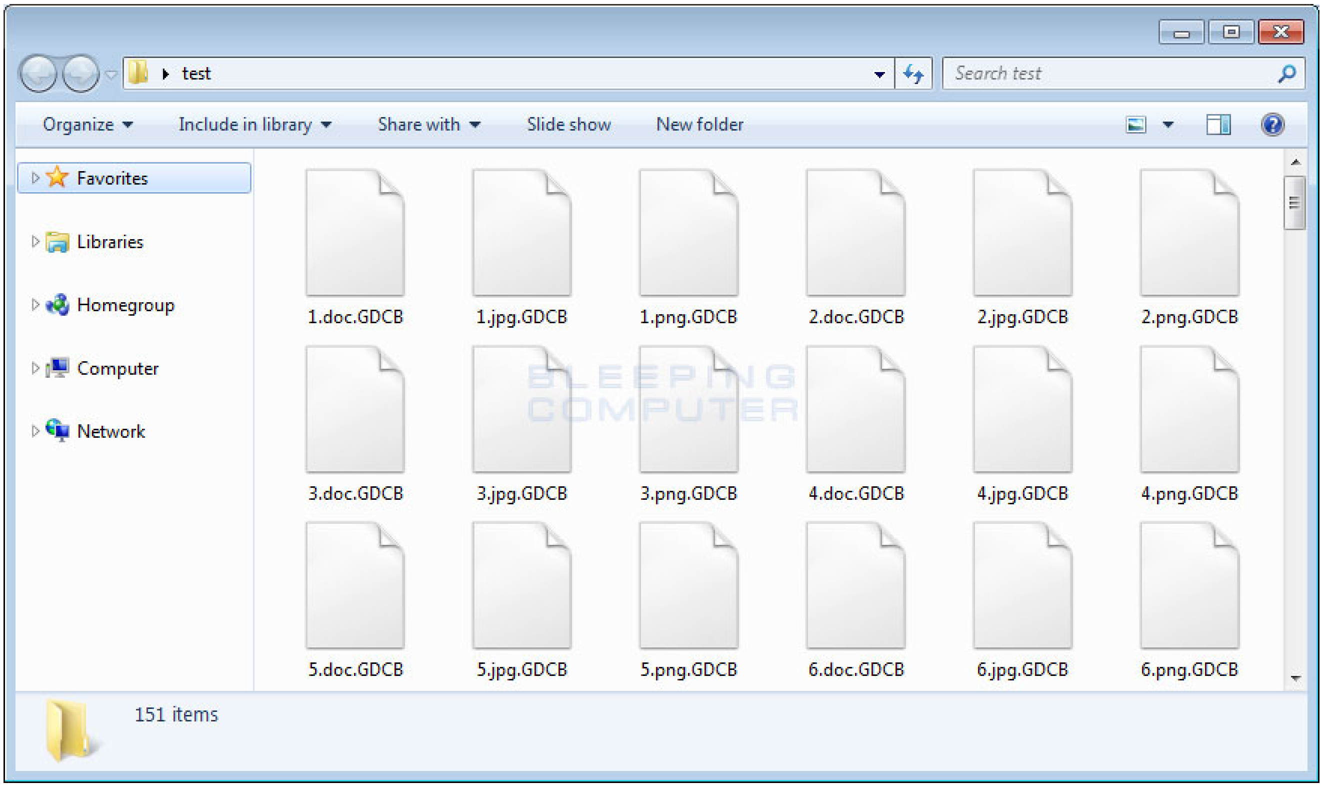
GandCrab will now begin to encrypt the victim's files and will target only certain file extensions. According to researcher Pepper Potts, the list of extensions are:

```
1cd, .3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .7z, .7zip, .aac, .ab4, .abd, .acc, .accdb,
.accde, .accdr, .accdt, .ach, .acr, .act, .adb, .adp, .ads, .agdl, .ai, .aiff, .ait,
.al, .aoi, .apj, .apk, .arw, .ascx, .asf, .asm, .asp, .aspx, .asset, .asx, .atb,
.avi, .awg, .back, .backup, .backupdb, .bak, .bank, .bay, .bdb, .bgt, .bik, .bin,
.bkp, .blend, .bmp, .bpw, .bsa, .c, .cash, .cdb, .cdf, .cdr, .cdr3, .cdr4, .cdr5,
.cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cfn, .cgm, .cib, .class, .cls, .cmt,
.config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cry, .cs, .csh, .csl, .css,
.csv, .d3dbsp, .dac, .das, .dat, .db, .db_journal, .db3, .dbf, .dbx, .dc2, .dcr,
.dcs, .ddd, .ddoc, .ddrw, .dds, .def, .der, .des, .design, .dgc, .dgn, .dit, .djvu,
.dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf,
.dxg, .edb, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla,
.flac, .flb, .flf, .flv, .flvv, .forge, .fpx, .fxg, .gbr, .gho, .gif, .gray, .grey,
.groups, .gry, .h, .hbk, .hdd, .hpp, .html, .ibank, .ibd, .ibz, .idx, .iif, .iiq,
.incpas, .indd, .info, .info_, .ini, .iwi, .jar, .java, .jnt, .jpe, .jpeg, .jpg, .js,
.json, .k2p, .kc2, .kdbx, .kdc, .key, .kpdx, .kwm, .laccdb, .lbf, .lck, .ldf, .lit,
.litemod, .litesql, .lock, .log, .ltx, .lua, .m, .m2ts, .m3u, .m4a, .m4p, .m4v, .ma,
.mab, .mapimail, .max, .mbx, .md, .mdb, .mdc, .mdf, .mef, .mfw, .mid, .mkv, .mlb,
.mmw, .mny, .money, .moneywell, .mos, .mov, .mp3, .mp4, .mpeg, .mpg, .mrw, .msf,
.msg, .myd, .nd, .ndd, .ndf, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf,
.nsg, .nsh, .nvram, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm,
.odp, .ods, .odt, .ogg, .oil, .omg, .one, .orf, .ost, .otg, .oth, .otp, .ots, .ott,
.p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pbf, .pcd, .pct, .pdb, .pdd, .pdf, .pef,
.pem, .pfx, .php, .pif, .pl, .plc, .plus_muhd, .pm!, .pm, .pmi, .pmj, .pml, .pmm,
.pmo, .pmr, .pnc, .pnd, .png, .pnx, .pot, .potm, .potx, .ppam, .pps, .ppsm,
.ppsx,.ppt, .pptm, .pptx, .prf, .private, .ps, .psafe3, .psd, .pspimage, .pst, .ptx,
.pub, .pwm, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .qcow, .qcow2, .qed, .qtb,
.r3d, .raf, .rar, .rat, .raw, .rdb, .re4, .rm, .rtf, .rvt, .rw2, .rwl, .rwz, .s3db,
.safe, .sas7bdat, .sav, .save, .say, .sd0, .sda, .sdb, .sdf, .sh, .sldm, .sldx, .slm,
.sql, .sqlite, .sqlite3, .sqlitedb, .sqlite-shm, .sqlite-wal, .sr2, .srb, .srf, .srs,
.srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stl, .stm, .stw, .stx,
.svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .tax, .tbb, .tbk, .tbn, .tex, .tga,
.thm, .tif, .tiff, .tlg, .tlx, .txt, .upk, .usr, .vbox, .vdi, .vhd, .vhdx, .vmdk,
.vmsd, .vmx, .vmxf, .vob, .vpd, .vsd, .wab, .wad, .wallet, .war, .wav, .wb2, .wma,
.wmf, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xls, .xlsb,
.xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xps, .xxx, .ycbcra, .yuv, .zip
```

While encrypting files, Kremez's analysis showed that GandCrab will skip any files whose full pathname contain the following strings:

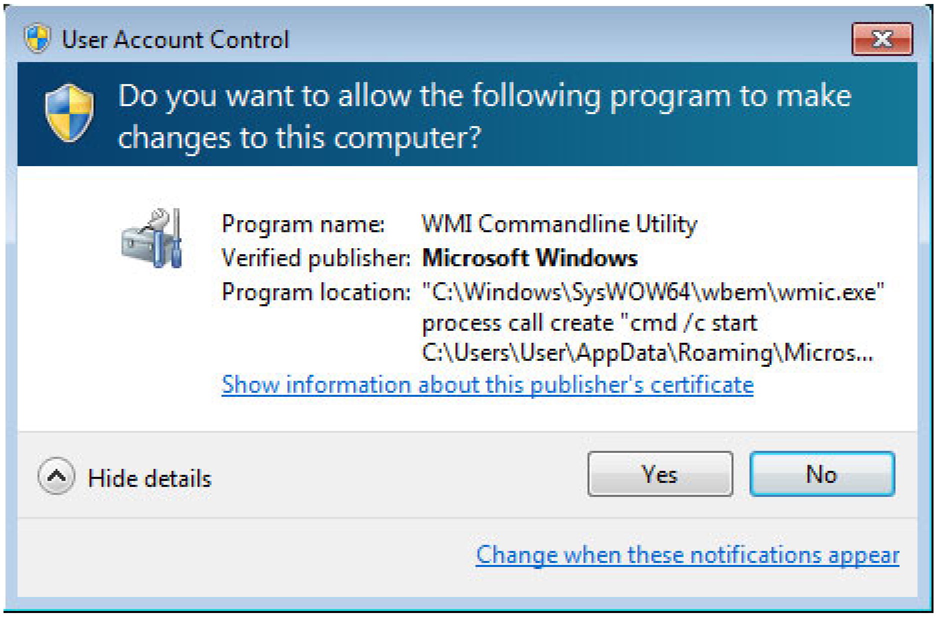
```
\ProgramData\, \Program Files\, \Tor Browser\, Ransomware, \All Users\, \Local
Settings\, desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.bak,
boot.ini, ntuser.dat.log, thumbs.db, GDCB-DECRYPT.txt, .sql
```

When encrypting files, the ransomware will append the **.GDCB** extension to the encrypted file's name. For example, test.jpg would be encrypted and renamed to test.jpg.GDCB.



Encrypted GDCB Files

At some point, the ransomware will relaunch itself using the command **"C:\Windows\system32\wbem\wmic.exe" process call create "cmd /c start %Temp%\[launched_file_name].exe"**. If a user does not respond Yes to the below prompt, it will continuously display the UAC prompt.



User Account Control

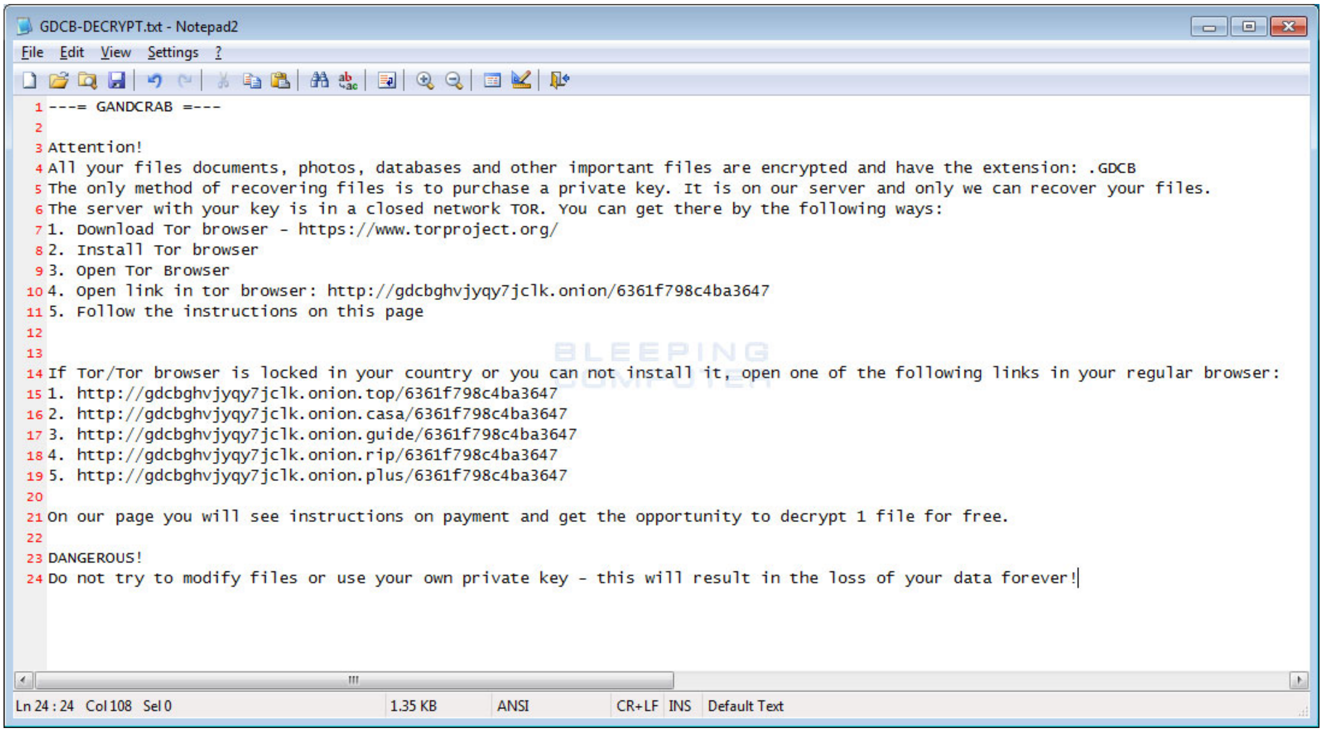
Do you want to allow the following program to make changes to this computer?

Program name: WMI Commandline Utility
Verified publisher: **Microsoft Windows**
Program location: "C:\Windows\SysWOW64\wbem\wmic.exe" process call create "cmd /c start C:\Users\User\AppData\Roaming\Micros...

Show information about this publisher's certificate
Hide details
Yes
No
Change when these notifications appear

UAC Prompt

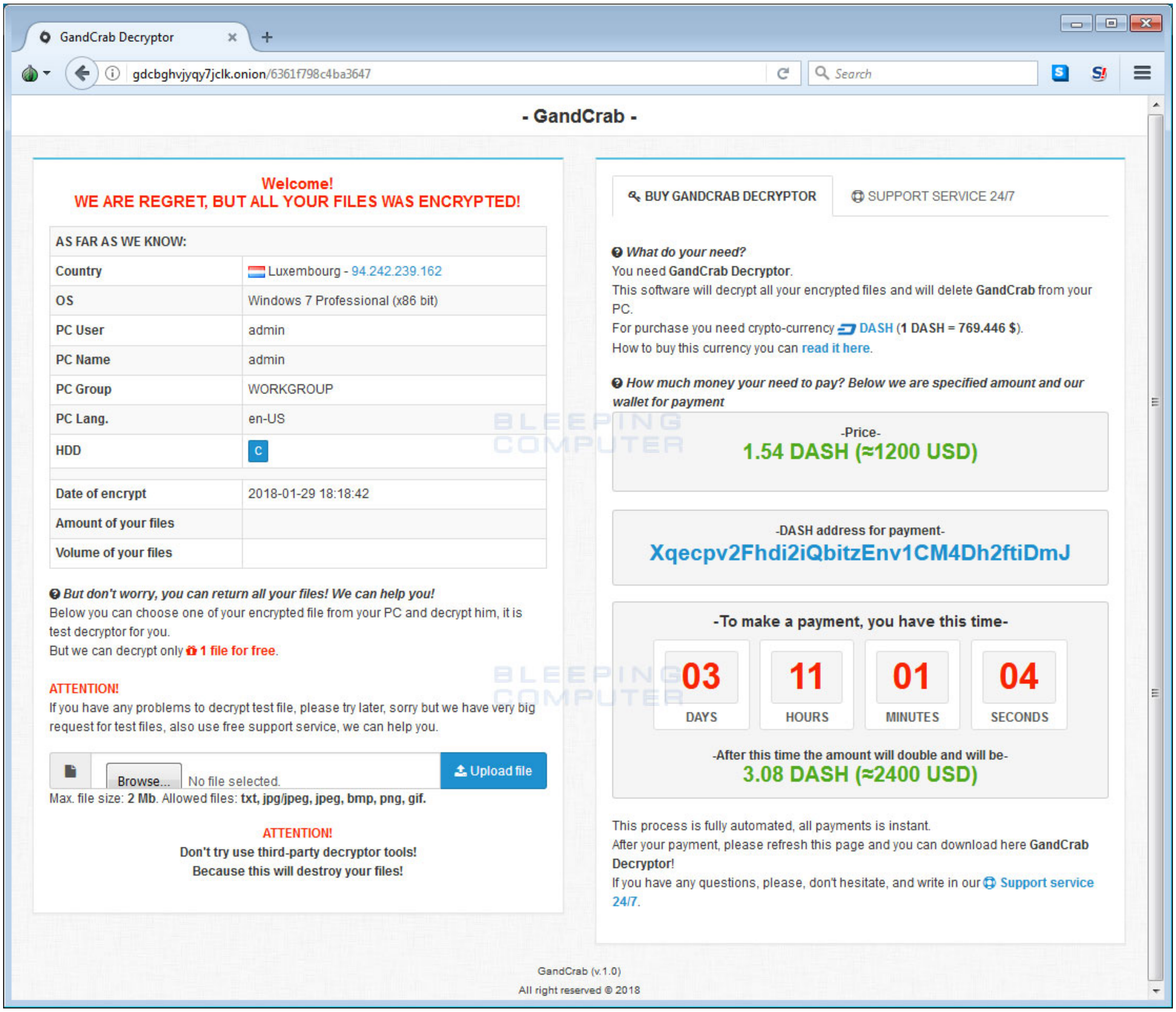
When the ransomware has finished encrypting the computer, victim's will find ransom notes located through the computer. This ransom note is named **GDCB-DECRYPT.txt** and contains information on what happened to the victim's files and a list of TOR gateways that can be used to access the payment site.



```
---= GANDCRAB =---

Attention!
All your files documents, photos, databases and other important files are encrypted and have the extension: .GDCB
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:
1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in tor browser: http://gdcbghvjyqy7jclk.onion/6361f798c4ba3647
5. Follow the instructions on this page


If Tor/Tor browser is locked in your country or you can not install it, open one of the following links in your regular browser:
1. http://gdcbghvjyqy7jclk.onion.top/6361f798c4ba3647
2. http://gdcbghvjyqy7jclk.onion.casa/6361f798c4ba3647
3. http://gdcbghvjyqy7jclk.onion.guide/6361f798c4ba3647
4. http://gdcbghvjyqy7jclk.onion.rip/6361f798c4ba3647
5. http://gdcbghvjyqy7jclk.onion.plus/6361f798c4ba3647

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

DANGEROUS!
Do not try to modify files or use your own private key - this will result in the loss of your data forever!
```

GandCrab GDCB-DECRYPT.txt Ransom Note

When a user goes to the listed site, they will be presented with a site called GandCrab Decryptor. This site provides information such as the ransom amount, the DASH address to send payment to, a support chat, and a free decryption of one file.



- GandCrab -

Welcome!
WE ARE REGRET, BUT ALL YOUR FILES WAS ENCRYPTED!

AS FAR AS WE KNOW:	
Country	Luxembourg - 94.242.239.162
OS	Windows 7 Professional (x86 bit)
PC User	admin
PC Name	admin
PC Group	WORKGROUP
PC Lang.	en-US
HDD	C
Date of encrypt	2018-01-29 18:18:42
Amount of your files	
Volume of your files	

But don't worry, you can return all your files! We can help you!
Below you can choose one of your encrypted file from your PC and decrypt him, it is test decryptor for you.
But we can decrypt only 1 file for free.

ATTENTION!
If you have any problems to decrypt test file, please try later, sorry but we have very big request for test files, also use free support service, we can help you.

Browse... No file selected. Upload file
Max. file size: 2 Mb. Allowed files: txt, jpg/jpeg, jpeg, bmp, png, gif.

ATTENTION!
Don't try use third-party decryptor tools!
Because this will destroy your files!

BUY GANDCRAB DECRYPTOR | SUPPORT SERVICE 24/7

What do your need?
You need **GandCrab Decryptor**.
This software will decrypt all your encrypted files and will delete **GandCrab** from your PC.
For purchase you need crypto-currency DASH (**1 DASH = 769.446 $**).
How to buy this currency you can read it here.

How much money your need to pay? Below we are specified amount and our wallet for payment

-Price-
1.54 DASH (≈1200 USD)

-DASH address for payment-
Xqecpv2Fhdi2iQbitzEnv1CM4Dh2ftiDmJ

-To make a payment, you have this time-

03	11	01	04
DAYS	HOURS	MINUTES	SECONDS

-After this time the amount will double and will be-
3.08 DASH (≈2400 USD)

This process is fully automated, all payments is instant.
After your payment, please refresh this page and you can download here **GandCrab Decryptor**!
If you have any questions, please, don't hesitate, and write in our Support service 24/7.

GandCrab (v.1.0)
All right reserved © 2018

GandCrab Decryptor

As already stated, unfortunately there is no way to decrypt the files for free at this time. If you need help or would like to discuss this ransomware, you can do so in our dedicated GandCrab Help & Support Topic.

How to protect yourself from the GandCrab Ransomware

In order to protect yourself from ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack. With a good backup, ransomware has no effect on you.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors and exploit kits. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Update 2/8/18 10:46 AM: Updated articles to include information from the NameCoin developers regarding how the GandCrab devs did not properly configure the C2 domains using NameCoin.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

GandCrab Hashes:

```
aedf80c426fb649bb258e430a3830d85
6866d8d8bf8565d94e0e1479978cf1e5
379e149517f4119f2edb9676ec456ed4
```

GandCrab Network Communication:

```
92.53.66.11/curl.php?token=
ipv4bot.whatismyipaddress.com
http://gdcbghvjyqy7jclk.onion
http://gdcbghvjyqy7jclk.onion.top/
http://gdcbghvjyqy7jclk.onion.casa/
http://gdcbghvjyqy7jclk.onion.guide/
http://gdcbghvjyqy7jclk.onion.rip/
http://gdcbghvjyqy7jclk.onion.plus/
```

GandCrab Files:

```
GDCB-DECRYPT.txt
```

GandCrab Ransom Note:

```
---= GANDCRAB =---

Attention!
All your files documents, photos, databases and other important files are encrypted
and have the extension: .GDCB
The only method of recovering files is to purchase a private key. It is on our server
and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the
following ways:
1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in tor browser: http://gdcbghvjyqy7jclk.onion/[id]
5. Follow the instructions on this page


If Tor/Tor browser is locked in your country or you can not install it, open one of
the following links in your regular browser:
1. http://gdcbghvjyqy7jclk.onion.top/[id]
2. http://gdcbghvjyqy7jclk.onion.casa/[id]
3. http://gdcbghvjyqy7jclk.onion.guide/[id]
4. http://gdcbghvjyqy7jclk.onion.rip/[id]
5. http://gdcbghvjyqy7jclk.onion.plus/[id]

On our page you will see instructions on payment and get the opportunity to decrypt 1
file for free.

DANGEROUS!
Do not try to modify files or use your own private key - this will result in the loss
of your data forever!
```

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-

  Demonslay335 - 4 years ago

  Excellent analysis by MalwareBytes here: https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/

  Seems to be secure unless network traffic was logged at time of infection.

-

  foxman751 - 4 years ago

  C:\Windows\system32\wbem\wmic.exe

  i can disaple wmic.exe like vssadmin.exe

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: