

"Proof of Concept" CryptoWire Ransomware Spawns Lomix and UltraLocker Families

bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

Catalin Cimpanu



By




[Catalin Cimpanu](#)

- December 9, 2016
- 02:31 PM
- 5

A new open-source ransomware project uploaded on GitHub as a "proof of concept," has now spawned three new ransomware families that are infecting users in real-life.

The original CryptoWire project was uploaded to GitHub by an anonymous user this past May.

The project, still available for download, contains a ZIP archive, with the ransomware's source code, and a README file advertising CryptoWire's capabilities.

Name	Type	Compressed size	Password ...	Size
 CryptoWire.au3	AU3 File	9 KB	No	
 includes.au3	AU3 File	5 KB	No	
 ransomware	TXT File	1 KB	No	

Contents of the CryptoWire package

According to its author, the ransomware is written in the Autolt scripting language and locks files stored on network drives, network shares, USB drives, external disks, internal disks, and cloud storage apps running on the machine such as Onedrive, Dropbox, Google Drive, and Steam.

CryptoWire uses the AES-256 algorithm for the encryption operations, which will encrypt all files smaller than 30MB (adjustable limit). The README file might have been outdated, as the ransomware's source code included file extension filters (pictured below).

```
Global $extensions_for_drives =
"zip|7z|rar|pdf|doc|docx|xls|xlsx|pptx|pub|one|vsdx|accdb|asd|xlsb|mdb|snp|wbk|ppt|psd|ai
|odt|ods|odp|odm|||odc|odb|docm|wps|xlsm|xlk|pptm|pst|dwg|dxf" & _

"dxg|wpd|rtf|wb2|mdf|dbf|pdd|eps|indd|cdr|dng|3fr|arw|srf|sr2|bay|crw|cr2|dcr|kdc|erf
|mef|mrw|nef|nrw|orf|raf|raw|rwl|rw2|r3d|ptx|pef|srw|x3f|der|" & _

"cer|crt|pem|pfx|p12|p7b|p7c|abw|til|aif|arc|as|asc|asf|ashdisc|asm|asp|aspx|asx|aup|
avi|bbb|bdb|bibtex|bkf|bmp|bpm|btd|bz2|c|cdi|himmel|cert|cfm|cgi" & _

"cpio|cpp|csr|cue|dds|dem|dmg|dsb|eddx|edoc|eml|emlx|EPS|epub|fdf|ffu|flv|gam|gcode|g
ho|gpx|gz|h|hbk|hdd|hds|hpp|ics|idml|iff|img|ipd|iso|isz|iwa" & _

"j2k|jp2|jpf|jpm|jpx|jsp|jspe|jspx|jst|key|keynote|kml|kmz|lic|lwp|lzma|M3U|M4A|m4v|m
ax|mbox|md2|mdbackup|mddata|mdinfo|mids|mid|mov|mp3|mp4|mpa|mpb|mpeg|mpg" & _

"mpj|mpp|msg|mso|nba|nbf|nbi|nbn|nbz|nco|nes|note|nrg|nri|afsnit|ogg|ova|ovf|oxps|p2i
|p65|p7|pages|pct|PEM|phtm|phtml|php|php3|php4|php5|phps|phpx|phpxx|pl|plist" & _

"pmd|pmx|ppdf|pps|ppsm|ppsx|ps|PSD|pspimage|pvm|qcn|qcow|qcow2|qt|ra|rm|rtf|s|sbf|set
|skb|slf|sme|smm|spb|sql|srt|ssc|ssi|stg|stl|svg|swf|sxw|syncdb|tager|tc|tex" & _

"tga|thm|tif|tiff|toast|torrent|txt|vbk|vcard|vcd|vcf|vdi|vfs4|vhd|vhdx|vmdk|vob|wbve
rify|wav|webm|wmb|wpb|WPS|xdw|xlr|XLSX|xz|yuv|zipx|jpg|jpeg|png|bmp"
```

The README claims the encryption process makes a copy of the targeted files, encrypts the copy, overwrites the original file ten times, and then permanently deletes its.

After the encryption process ends, CryptoWire will delete all shadow volume copies, and overwrite the content of the RecycleBin ten times and permanently delete it.

When displaying the ransom note, CryptoWire will check if the infected target is part of a domain and multiply the ransom demand by 10 (adjustable value).

CryptoWire's author said it shipped the ransomware without a backend panel "to prevent skids from abusing it." Unfortunately, skids abused it.

Real-life CryptoWire spawns

The first CryptoWire spawn was detected at the end of October by GData malware analyst [Karsten Hahn](#), using the same name: CryptoWire.

This version appears to have been under development, as one crucial button for the decryption process was missing from its interface.

Your files has been safely encrypted

Encrypted files: 0



Buy Bitcoins

Decrypt Files

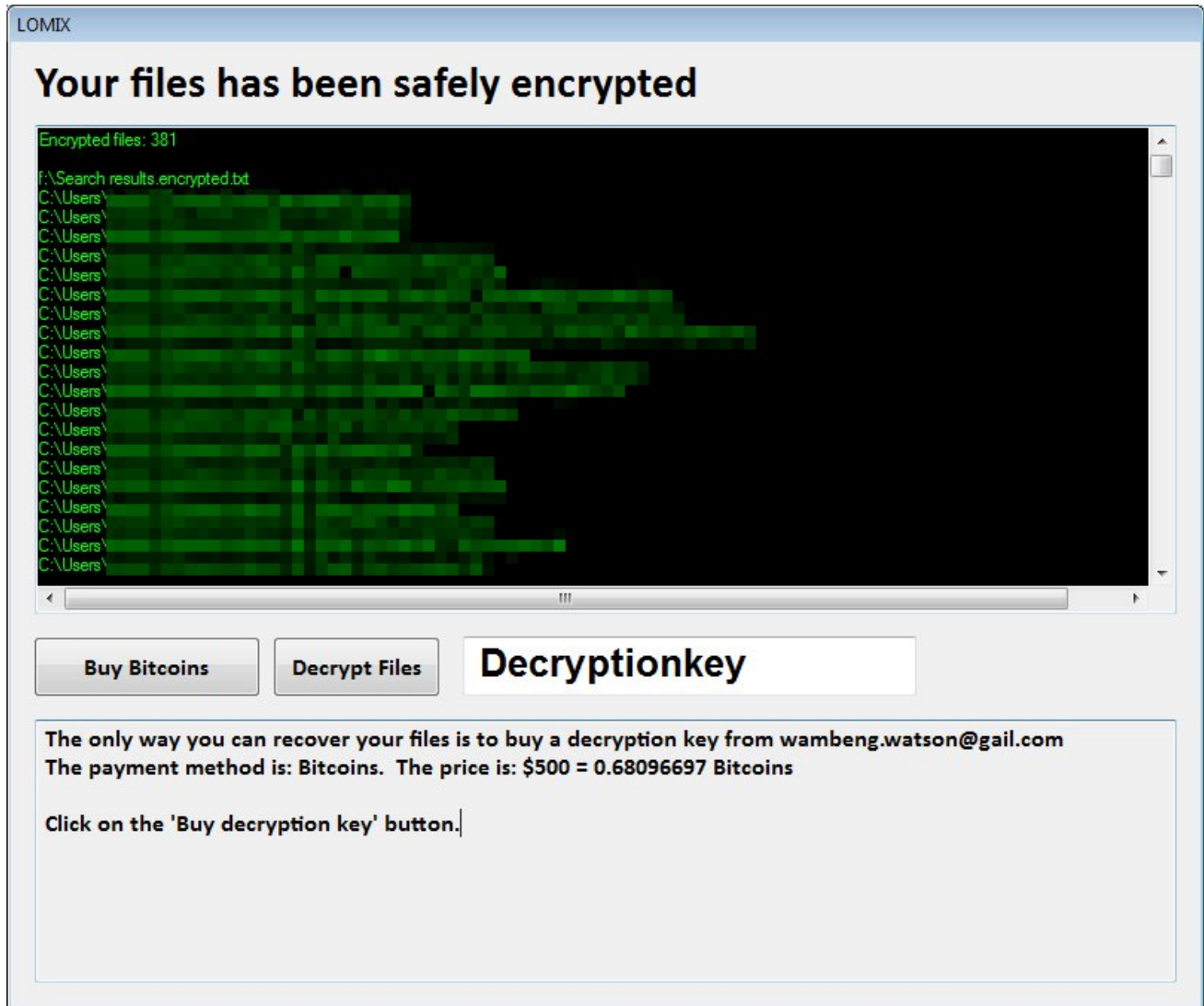
Decryptionkey

The only way you can recover your files is to buy a decryption key
The payment method is: Bitcoins. The price is: \$200 = Bitcoins

Click on the 'Buy decryption key' button.

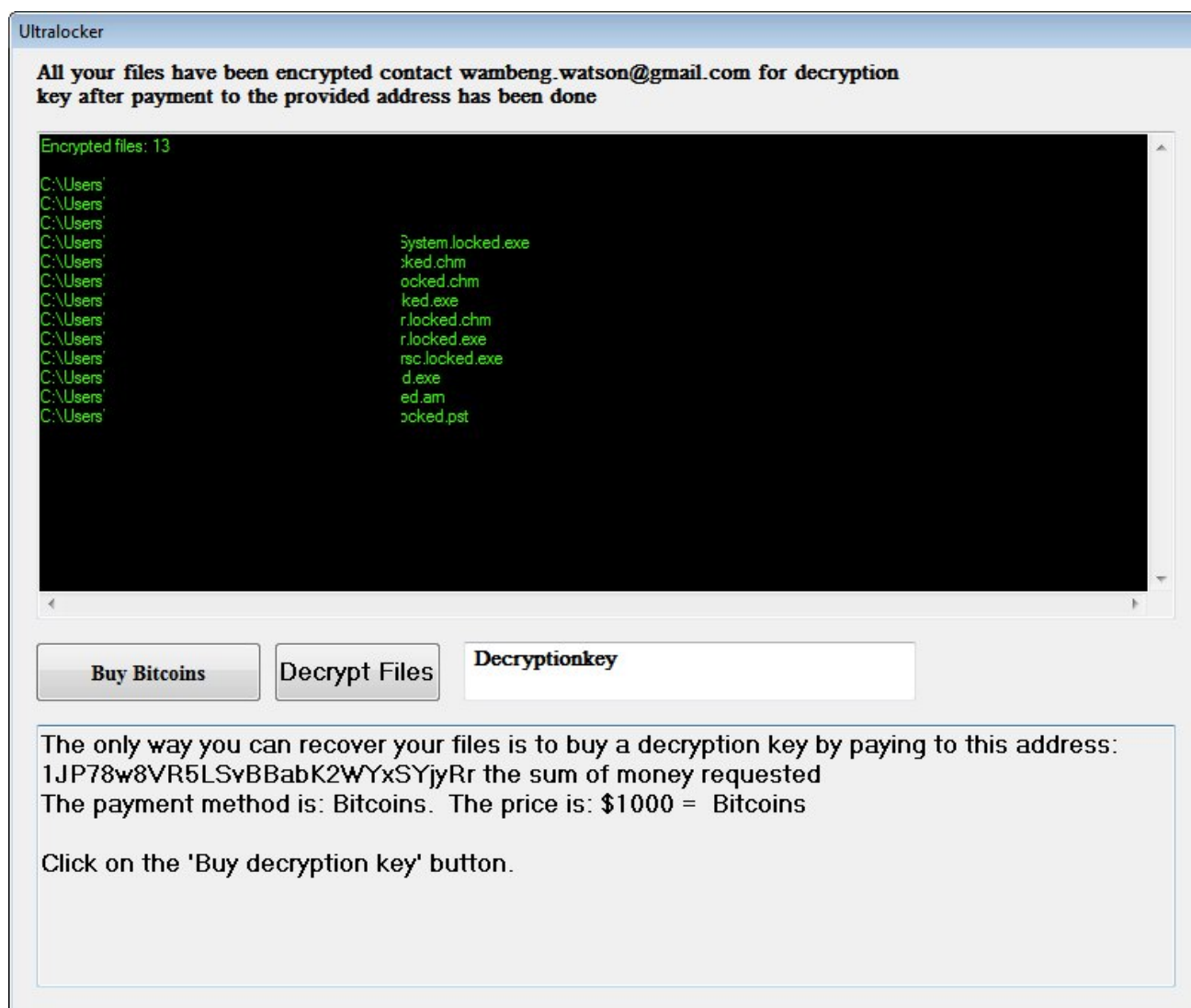
CryptoWire variant, October 2016

A month later, security researcher [S!Ri](#) discovered the Lomix ransomware, pictured below.



Lomix ransomware, November 2016

Today, the same Karsten Hahn has come across another CryptoWire variant that goes by the name of UltraLocker and spreads a spam campaign delivering malicious Word files.



UltraLocker ransomware, December 2016

The problem of open-source and so-called "educational" ransomware has been discussed in the past numerous times. Previous open-source ransomware families included Hidden Tear, EDA2, [CryptoTrooper](#), and [Heimdall](#).

In all cases, the authors of these projects have hidden from any responsibility and damage their code would have caused just by using words as "educational" and "proof of concept," not realizing that real-life malware coders don't care.

Most crooks look at open-source ransomware as free work, and hours of work they don't have to put in designing, documenting, and writing their own code. How about we stop giving crooks a helping hand, shall we?

Related Articles:

[BlackCat/ALPHV ransomware asks \\$5 million to unlock Austrian state](#)

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[Hacker says hijacking libraries, stealing AWS keys was ethical research](#)

- [CryptoWire](#)
- [Lomix](#)
- [Open Source](#)
- [Ransomware](#)
- [UltraLocker](#)

[Catalin Cimpanu](#)

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campusodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- [Previous Article](#)
- [Next Article](#)

Comments



Uselesslight - 5 years ago

-
-

Or alternatively Catalin, why don't we not stop "helping" crooks? I see the points you're making, and they are concise and accurate, but on the other hand: Do you not feel that the masses need education, on all topics? Understandable that so-called crooks are going to try and repurpose these types of software, why would they not? However, this is a byproduct of education, we have schools that teach people about bombs, why do they not get told to stop helping the crooks? People can utilize this knowledge for very good purposes, like all things. I strongly feel that these open source ransomware's popping up periodically could turn out being more beneficial, if more people familiarize themselves with the concepts, two things could potentially happen. 1) People are going to garnish more awareness on security issues such as these and having a working proof-of-concept will make it easier to educate people who are misinformed. 2) More knowledge of ransomware in general is made possible by this. Would it not be great, if encryption as it is became a common understanding and the issues like ransomware would go away? Think of the possibilities if everyone was capable of decrypting their files following a ransomware infection? Also, the so-called crooks utilizing open-source software, are DEFINITELY not the ones that are going to be causing serious damages... Of course though, I do see your point on the matter, but this is just another take on that.



• Struppigel - 5 years ago

-
-

"Also, the so-called crooks utilizing open-source software, are DEFINITELY not the ones that are going to be causing serious damages..."

Have you ever had a look at the forums for the help request to all the HiddenTear/EDA2 variants? They are causing major damage to people and organizations.

Me and some of my colleagues have written articles about that matter, because it is discussed a lot lately. If you are interested in our reasoning, you might want to read that: <https://blog.gdatasoftware.com/2016/11/29289-it-s-educational-on-the-no-1-argument-for-open-source-ransomware>



• Uselesslight - 5 years ago

-
-

Certainly I will have a read through your publication. Don't get me wrong, I'm not trying to say "my way or the highway". I just see the value in learning this kind of stuff.



Amigo-A - 5 years ago

-
-

HiddenTear/EDA2 or CryptoWire...

It's like, what produce grenades, bombs and deadly weapons, and then cry out for mercy.

If you made a bombshell, If put it in the wrong hands - it will fly and explode, what to cause injury and death.



Uselesslight - 5 years ago

-
-

That is kind of my point Amigo-A, everything that has ever been created, ever has the potential of being misused. It's going to exist one or another though, there is nothing we can do, at this point the lesser of two evils is to embrace it and learn as much as we can. The only hope we have against ransomware it seems is education now.

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:
