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

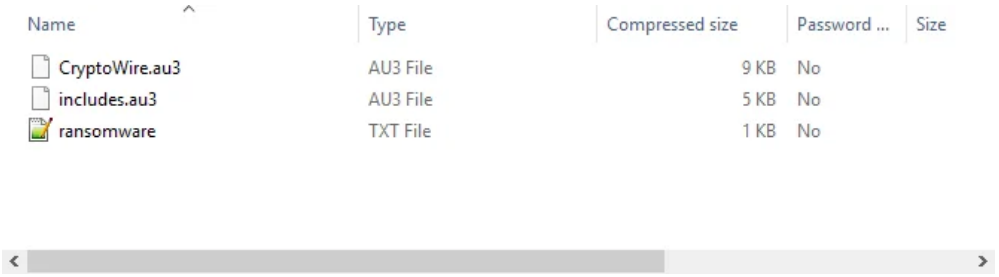
By Catalin Cimpanu

Published: 2016-12-09 · Archived: 2026-04-05 19:08:42 UTC

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.

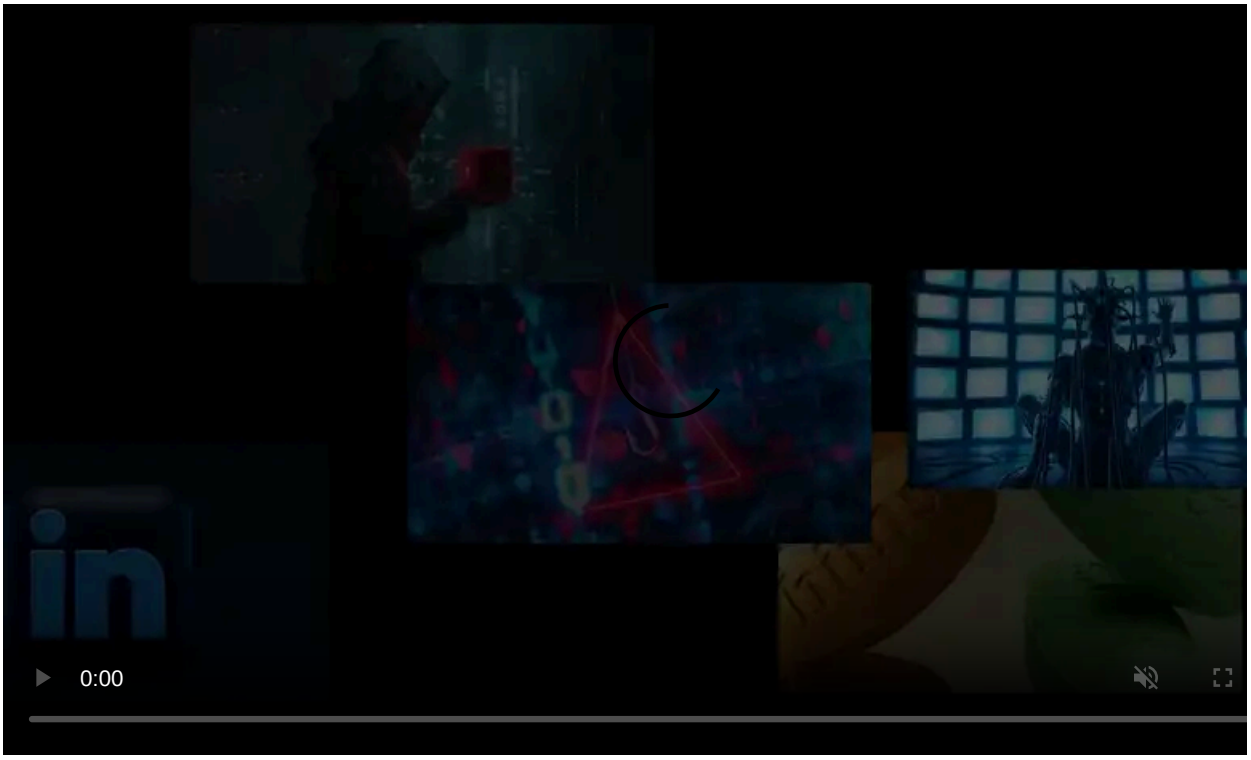
The project, still available for download, contains a ZIP archive, with the ransomware's source code, and a README file advertising CryptoWire's capabilities.

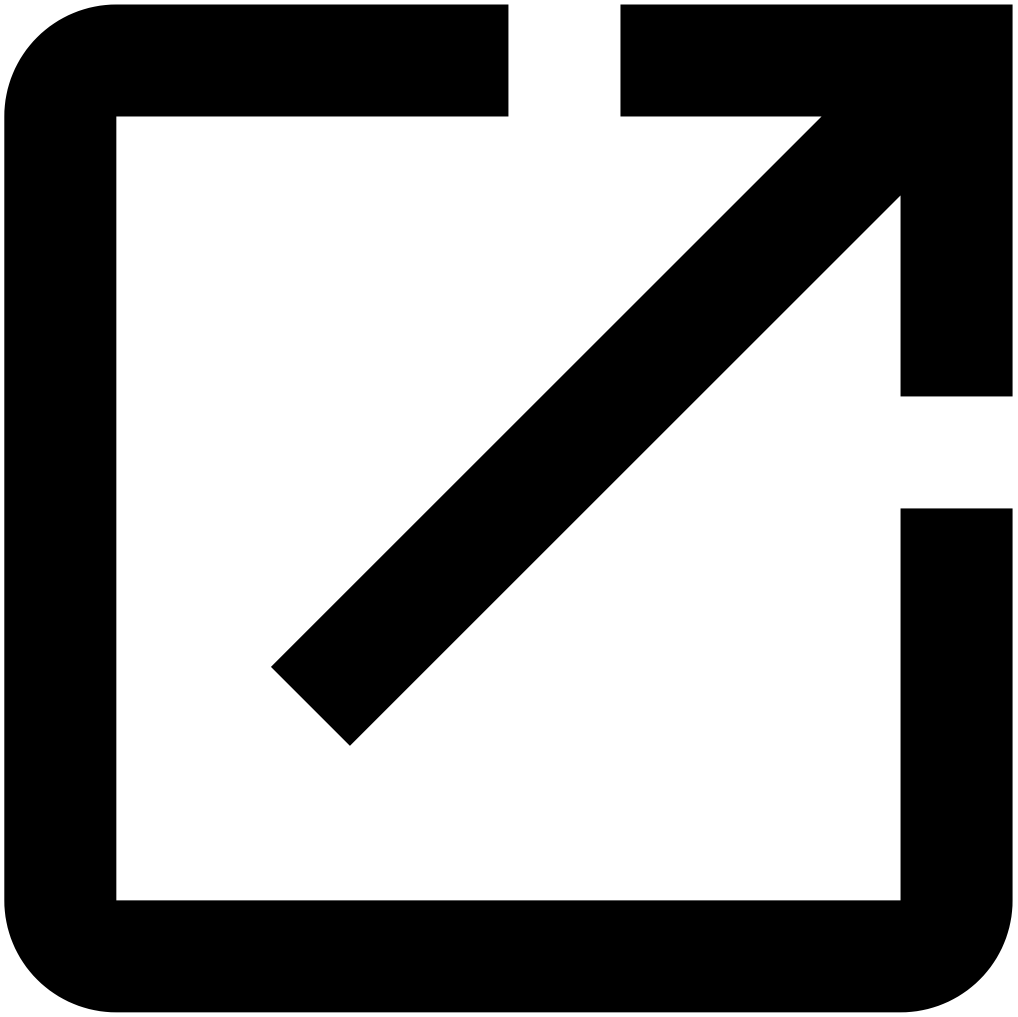


Name	Type	Compressed size	Password ...	Size
CryptoWire.au3	AU3 File	9 KB	No	
includes.au3	AU3 File	5 KB	No	
ransomware	TXT File	1 KB	No	

Contents of the CryptoWire package

According to its author, the ransomware is written in the AutoIt 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.


0:00



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 The README file might have been outdated, as the ransomware's source code included file extension filters (pictured below).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|bpn|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|jspa|jspx|jst|key|keynote|kml|kmz|lic|lwp|lzma|M3U|M4A|m4v|m
    ax|mbox|md2|mdbackup|mddata|mdinfo|mds|mid|mov|mp3|mp4|mpa|mpb|mpeg|mpg" & _

    "mpj|mpp|msg|mso|nba|nbf|nbi|nbu|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.

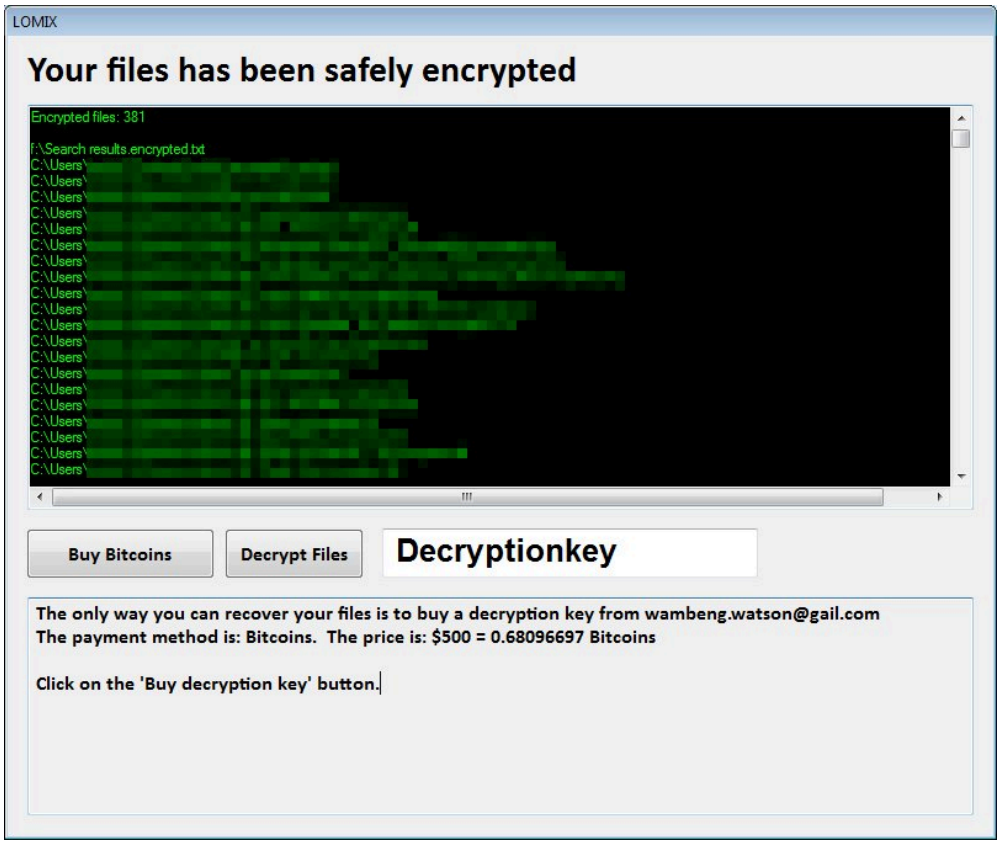
Real-life CryptoWire spawns

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.

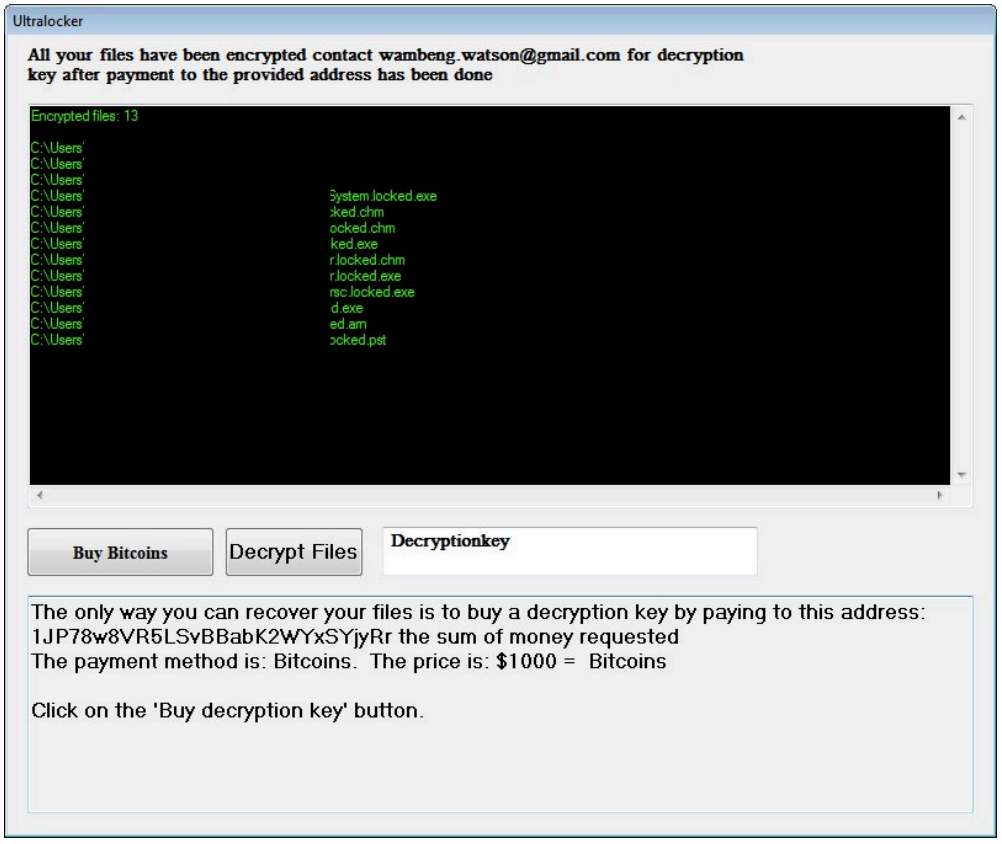
CryptoWire variant, October 2016

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.

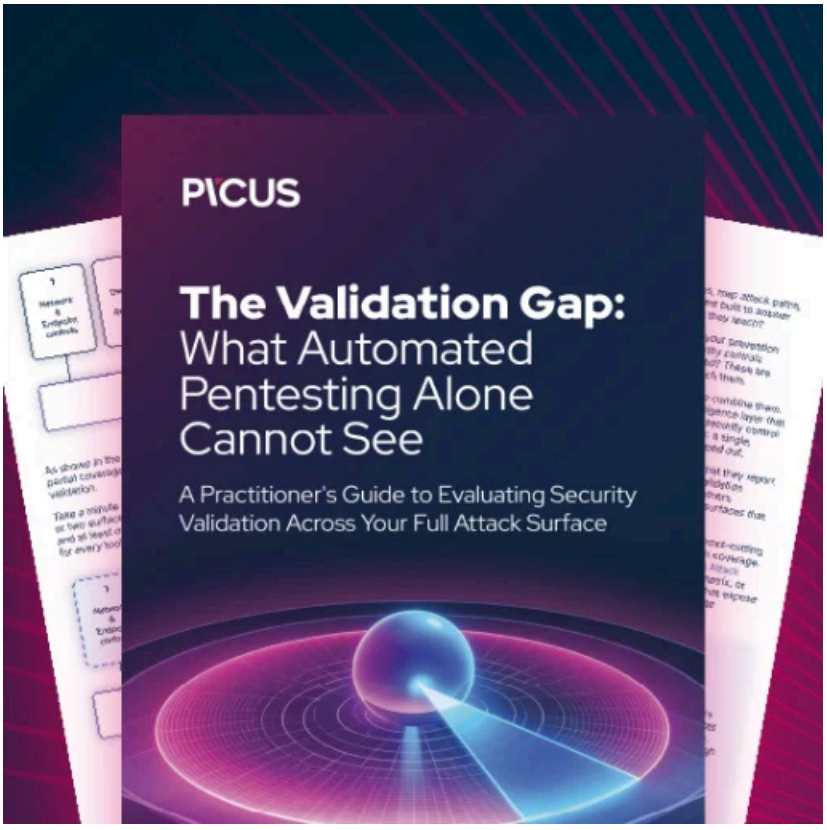


UltraLocker ransomware, December 2016

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?



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/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/