

# Maktub ransomware: possibly rebranded as Iron

Archived: 2026-04-06 01:08:38 UTC

In this post, we'll take a quick look at a possible new ransomware variant, which appears to be the latest version of Maktub ransomware, also known as Maktub Locker.

[Hasherazade](#) from Malwarebytes has, as per usual, written an excellent blog on Maktub Locker in the past, if you wish to learn more: [Maktub Locker – Beautiful And Dangerous](#)

**Update - 2018-04-14:** Read the conclusion at the end of this post to learn more about how Iron ransomware mimicked at least three different ransomware families.

## Analysis

A file was discovered, named *ado64* with the following properties:

- **MD5:** 1e60050db59e3d977d2a928fff3d34a6
- **SHA1:** f51bab89b4e4510b973df8affc2d11a4476bd5be
- **SHA256:** 19ee6d4a89d7f95145660ca68bd133edf985cc5b5c559e7062be824c0bb9e770
- **Compilation timestamp:** 2018-04-05 03:47:19
- **VirusTotal report:**  
[19ee6d4a89d7f95145660ca68bd133edf985cc5b5c559e7062be824c0bb9e770](#)

Maktub typically sports a graphically appealing lock screen, as well as payment portal, and promotes "Maktub Locker" extensively.

Interestingly enough, this variant has removed all references to Maktub. The figures below represent lock screen and payment portal, when stepping through.



Figure 1 - Lock screen/warning

Email address: *recoverfile@mail2tor.com*

Bitcoin address: *1cimKyzS64PRNEiG89iFU3qzckVuEQUj*

Ransomware note: *!HELP\_YOUR\_FILES.HTML*

Enter your personal ID here:

Submit

Figure 2 - Payment portal

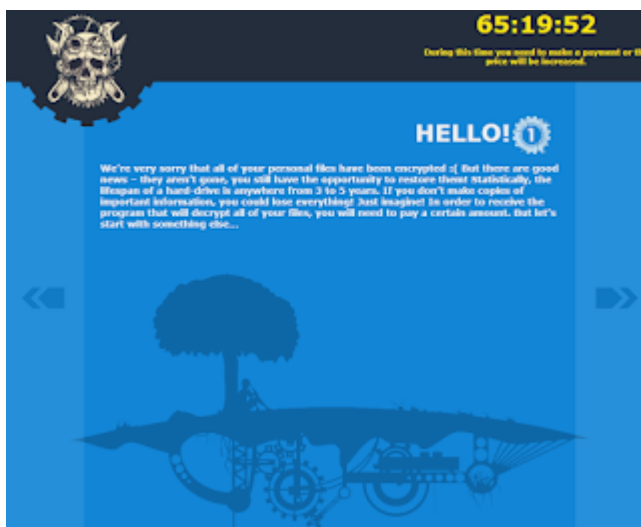


Figure 3 - Hello! (after entering the personal ID)

The text reads:

*We're very sorry that all of your personal files have been encrypted :( But there are good news – they aren't gone, you still have the opportunity to restore them! Statistically, the lifespan of a hard-drive is anywhere from 3 to 5 years. If you don't make copies of important information, you could lose everything! Just imagine! In order to receive the program that will decrypt all of your files, you will need to pay a certain amount. But let's start with something else...*

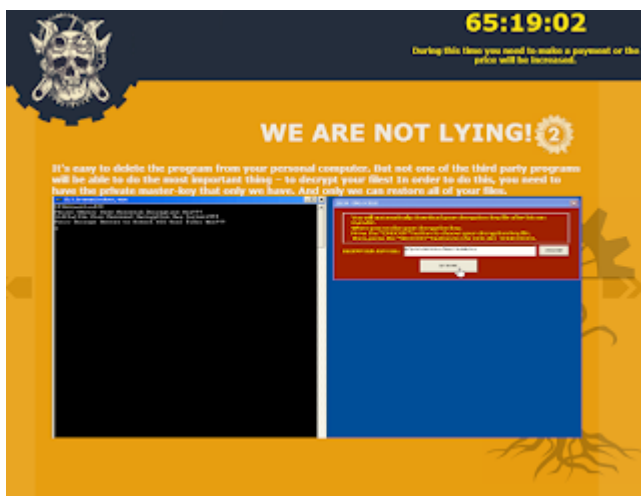


Figure 4 - "We are not lying"



Figure 5 - Ransomware cost



Figure 6 - Where to pay

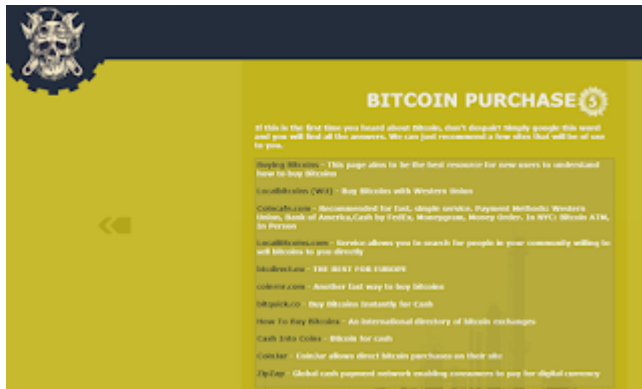


Figure 7- Last but not least: how to buy Bitcoins

In previous versions of Maktub, you could decrypt 1 file for free, however, with the current rebranding, this option has disappeared. Since the ransomware has rebranded, we'll name it "Iron" or "Iron ransomware", due to the name of the decrypter, *IronUnLocker*.

Iron encrypts a whopping total of **374** extensions, these are as follows:

.001, .1cd, .3fr, .8ba, .8bc, .8be, .8bf, .8bi8, .8bl, .8bs, .8bx, .8by, .8li, .DayZProfile, .abk, .ade, .adpb, .adr, .aip, .amxx, .ape, .api, .apk, .arch00, .aro, .arw, .asa, .ascx, .ashx, .asmx, .asp, .asr, .asset, .bar, .bay, .bc6, .bc7, .bi8, .bic, .big, .bin, .bkf, .bkp, .blob, .blp, .bml, .bp2, .bp3, .bpl, .bsa, .bsp, .cab, .cap, .cas, .ccd, .cch, .cer, .cfg, .cfr, .cgf, .chk, .class, .clr, .cms, .cod, .col, .con, .cpp, .cr2, .crt, .crw, .csi, .cso, .css, .csv, .ctt, .cty, .cwf, .d3dbsp, .dal, .dap, .das, .db0, .dbb, .dbf, .dbx, .dcp, .dcr, .dcu, .ddc, .ddcx, .dem, .der, .desc, .dev, .dex, .dic, .dif, .dii, .disk, .dmg, .dmp, .dob, .dox, .dpk, .dpl, .dpr, .dsk, .dsp, .dvd, .dxg, .elf, .epk, .eql, .erf, .esm, .f90, .fcd, .fla, .flp, .for, .forge, .fos, .fpk, .fpp, .fsh, .gam, .gdb, .gho, .grf, .h3m, .h4r, .hkdb, .hxx, .hplg, .htm, .html, .hvpl, .ibank, .icxs, .img, .indd, .ipa, .iso, .isu, .isz, .itdb, .itm, .itm, .iwd, .iwi, .jar, .jav, .java, .jpe, .kdc, .kmz, .layout, .lbf, .lbi, .lcd, .lcf, .ldb, .ldf, .lgp, .litemod, .lng, .lrf, .ltm, .ltx, .lvl, .m3u, .m4a, .map, .mbx, .mcd, .mcgame, .mcmeta, .md0, .md1, .md2, .md3, .mdb, .mdbackup, .mddata, .mdf, .mdl, .mdn, .mdu, .mef, .menu, .mm6, .mm7, .mm8, .moz, .mpq, .mpqge, .mrwref, .mxp, .ncf, .nds, .nrg, .nri, .nrw, .ntl, .odb, .odf, .odp, .ods, .odt, .orf, .owl, .oxt, .p12, .p7b, .p7c, .pab, .pbp, .pef, .pem, .pfx, .pkb, .pkh, .pkpass, .plc, .pli, .pot, .potm, .potx, .ppf, .ppsm, .pptm, .prc, .prt,

.psa, .pst, .ptx, .pww, .pxp, .qbb, .qdf, .qel, .qic, .qpx, .qtr, .r3d, .raf, .re4, .res, .rgn, .rgss3a, .rim, .rofl, .rrt, .rsrc, .rsw, .rte, .rw2, .rwl, .sad, .sav, .sc2save, .scm, .scx, .sdb, .sdc, .sds, .sdt, .shw, .sid, .sidd, .sidn, .sie, .sis, .slm, .slt, .snp, .snx, .spr, .sql, .sr2, .srf, .srw, .std, .stt, .sud, .sum, .svg, .svr, .swd, .syncdb, .t01, .t03, .t05, .t12, .t13, .tar.gz, .tax, .tcx, .thmx, .tlz, .tor, .torrent, .tpu, .tpx, .ttarch2, .tur, .txd, .txf, .uax, .udf, .umx, .unity3d, .unr, .uop, .upk, .upoi, .url, .usa, .usx, .ut2, .ut3, .utc, .utx, .uvx, .uxx, .vcd, .vdf, .ver, .vfs0, .vhd, .vmf, .vmt, .vpk, .vpp\_pc, .vsi, .vtf, .w3g, .w3x, .wad, .war, .wb2, .wdgt, .wks, .wmdb, .wmo, .wotreplay, .wpd, .wpl, .wps, .wtd, .wtf, .x3f, .xla, .xlam, .xlc, .xll, .xlm, .xlr, .xlsb, .xltx, .xlv, .xlwx, .xpi, .xpt, .yab, .yps, .z02, .z04, .zap, .zipx, .zoo, .ztmp

Iron doesn't spare gamers, as it will also encrypt Steam files (.vdf), World of Tanks replays (.wotreplay). DayZ (.DayZProfile), and possibly others.

Folders containing the following words are exempt from encryption:

Windows, windows, Microsoft, Mozilla Firefox, Opera, Internet Explorer, Temp, Local, LocalLow, \$Recycle.bin, boot, i386, st\_v2, intel, recycle, 360rec, 360sec, 360sand, internet explorer, msbuild

Interestingly enough, 360sec, 360rec, and 360sand is developed by Qihoo 360, an internet security company based in China, and is an antivirus (360 Total Security is one example). This, as well as the fact that the Iron ransomware also includes resources in Chinese Simplified, alludes this variant may be developed by a Chinese speaker.

The ransomware will additionally delete the original files after encryption, and will also empty the recycle bin. It does **not** remove Shadow Volume Copies or Restore Points.

Iron embeds a public RSA key as follows:

-----BEGIN RSA PUBLIC KEY-----  
MIGJAoGBAIOYf0KqEOGaxdLmMLypMyZ1q/K+r6DuCdYpwZfs0EPug3ye7UjZa0QMOP5/OySr  
/uBJtkmEghEtUEo/zfcBJ7332O1ytJ7/ebIUv+ZcN1Rlswzdv7uZxYRC8u1HvrgBvAz4Atb  
zx+FbFVqLB0gGixYTqbjqANq21AR6r91+oJtAgMBAAE=  
-----END RSA PUBLIC KEY-----

The Iron ransomware will determine the user's WAN IP and also send a POST request to its C2 server, [http://y5mogzal2w25p6bn\[.\]jml](http://y5mogzal2w25p6bn[.]jml).



Figure 8 - Traffic

It appears Iron will create a new, random GUID, and use it as a mutex, in order to not infect the machine twice. The following values will be sent to the C2:

- Encryption key;
- Randk (seed);
- GUID (mutex);
- Start (whether ransom successfully started);
- Market (unknown).

The C2 server will then respond with another set of values, and generate a *unique* Bitcoin address, which means that victims may pay twice to different addresses. Rule of thumb: do **not** pay the ransomware.

Of note is an email address in the response: *oldblackjack@outlook.com*.

Iron will additionally save certain values, such as the GUID, in *HKCU\Software\CryptoA*:



Figure 9 - Registry values (click to enhance)

Encrypted files will have the **.encry** extension appended. It is likely not possible to restore data.

### Conclusion

It is currently unknown if Iron is indeed a new variant by the same creators of Maktub, or if it was simply inspired by the latter, by copying the design for the payment portal for example.

We know the Iron ransomware has mimicked at least three ransomware families:

- **Maktub** (payment portal design)
- **DMA Locker** (Iron Unlocker, decryption tool)
- **Satan** (exclusion list)

From the screenshots above, it is obvious the portal design has been copy pasted from Maktub.

As for copying from DMA Locker, see this tweet:

And, last but not least, it uses the exact same exclusion list (folders and its content that will *not* be encrypted) from Satan:

Just to clarify, there isn't specific code overlap, as the crypto is quite different to Satan. However, there are similarities in a number of things, such as the exclusion list. <https://t.co/OHkFimJ3gZ>  
[pic.twitter.com/ub6hOnucgn](https://t.co/OHkFimJ3gZ)  
— Bart (@bartblaze) [April 11, 2018](#)

Code is indeed quite unique, and Iron seems like a totally new ransomware, and may even be a "side project" by the creators of the Satan ransomware. However, at this point, there is no sure way of telling who's behind Iron. Time may be able to tell.

**Decryption** is impossible without the author's private key, however, it is possible to restore files using Shadow Volume Copies, or alternatively [Shadow Explorer](#). If that doesn't work, you may try using a data recovery program such as [PhotoRec](#) or [Recuva](#).

Take note of [ID ransomware](#), if a decryptor should ever become available. Additionally, it may identify other families of ransomware if you are ever affected. Another service to take note of in this regard is [NoMoreRansom](#).

For preventing ransomware, have a look here:

In short: **create backups!**

Questions, comments, feedback or help: leave a comment below or contact me on [Twitter](#).

**Indicators:**

Indicator type	Indicator
email	oldblackjack@outlook.com
domain	y5mogzal2w25p6bn.ml
FileHash-SHA256	19ee6d4a89d7f95145660ca68bd133edf985cc5b5c559e7062be824c0bb9e770
URL	http://y5mogzal2w25p6bn.ml
URL	http://y5mogzal2w25p6bn.ml/receive
FileHash-MD5	1e60050db59e3d977d2a928fff3d34a6
FileHash-SHA1	f51bab89b4e4510b973df8affc2d11a4476bd5be
email	recoverfile@mail2tor.com

On AlienVault:

---

Source: <https://bartblaze.blogspot.de/2018/04/maktub-ransomware-possibly-rebranded-as.html>