EMSISOFT Blog

Decrypt latest Nemucod ransomware with Emsisoft's free decrypter

In Emsisoft Lab by Holger on July 12, 2017 | English

Update (July 16th, 2017):

Shortly before we published our article, the NemucodAES threat actors unleashed a new version of their ransomware that wasn't supported by our original decrypter. We are happy to announce that version 1.0.0.54 and later of our decrypter support this new version now. If you have tried the decrypter before unsuccessfully please download and try it again. Thanks!

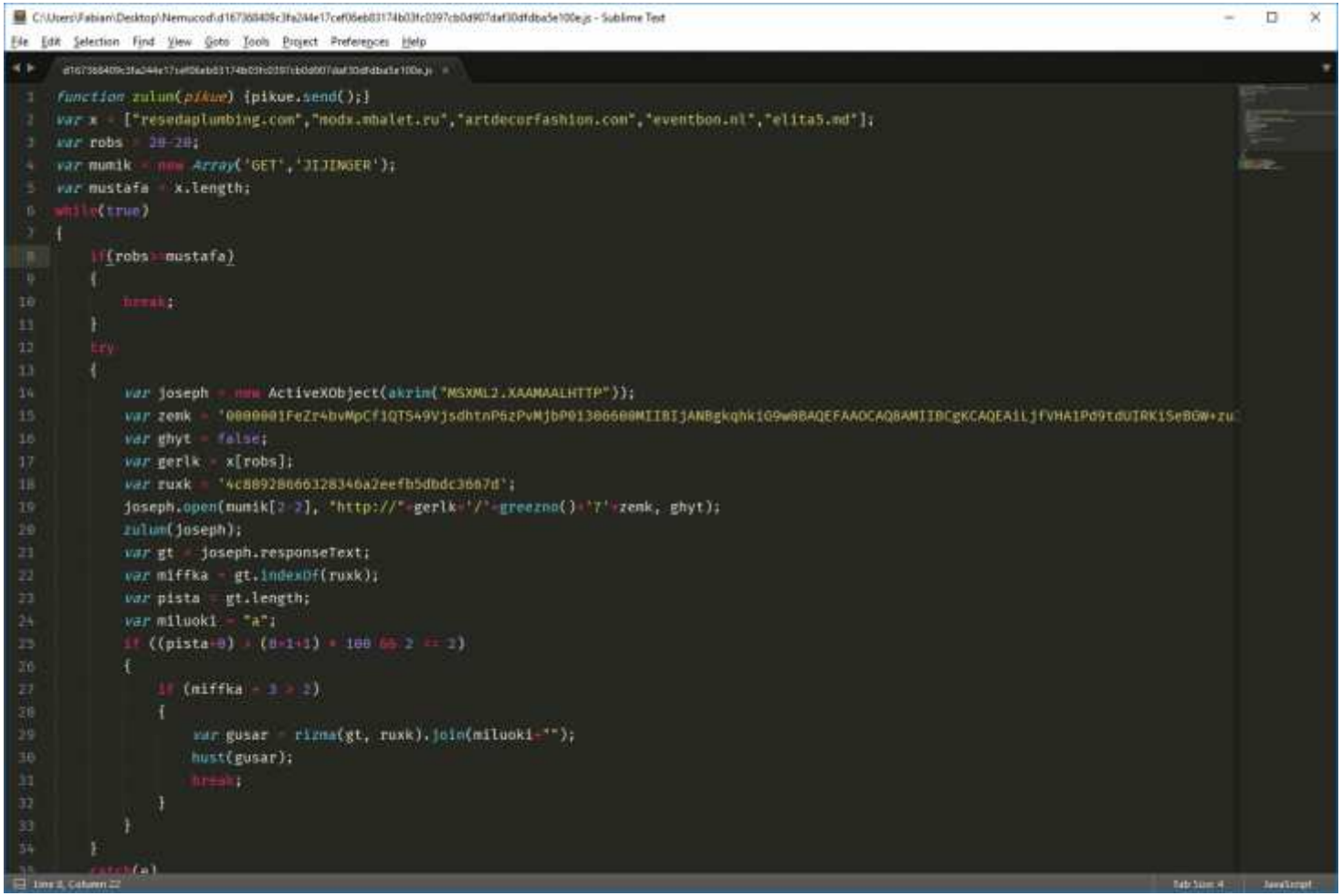
The Nemucod ransomware family has been around for a while and has gone through several evolutions and changes since then. Previous attempts of extorting money were thwarted by the release of our decrypter to help victims release their files for free.

Amidst the noise of the NotPetya ransomware outbreak, a new variant of Nemucod dubbed NemucodAES was released that made changes to the encryption mechanism as well as introduced a facelift of its ransom note.

Not to be outplayed by cyber criminals our lab promptly went to work and produced a new version of our decrypter to handle NemucodAES and free victim's files.

How NemucodAES ransomware works

The main infection vector of this latest offspring of the Nemucod ransomware family has remained the same, relying on the classic 'undelivered package' spam campaign to trick victims to click on the contained attachment and execute the JavaScript contained within.

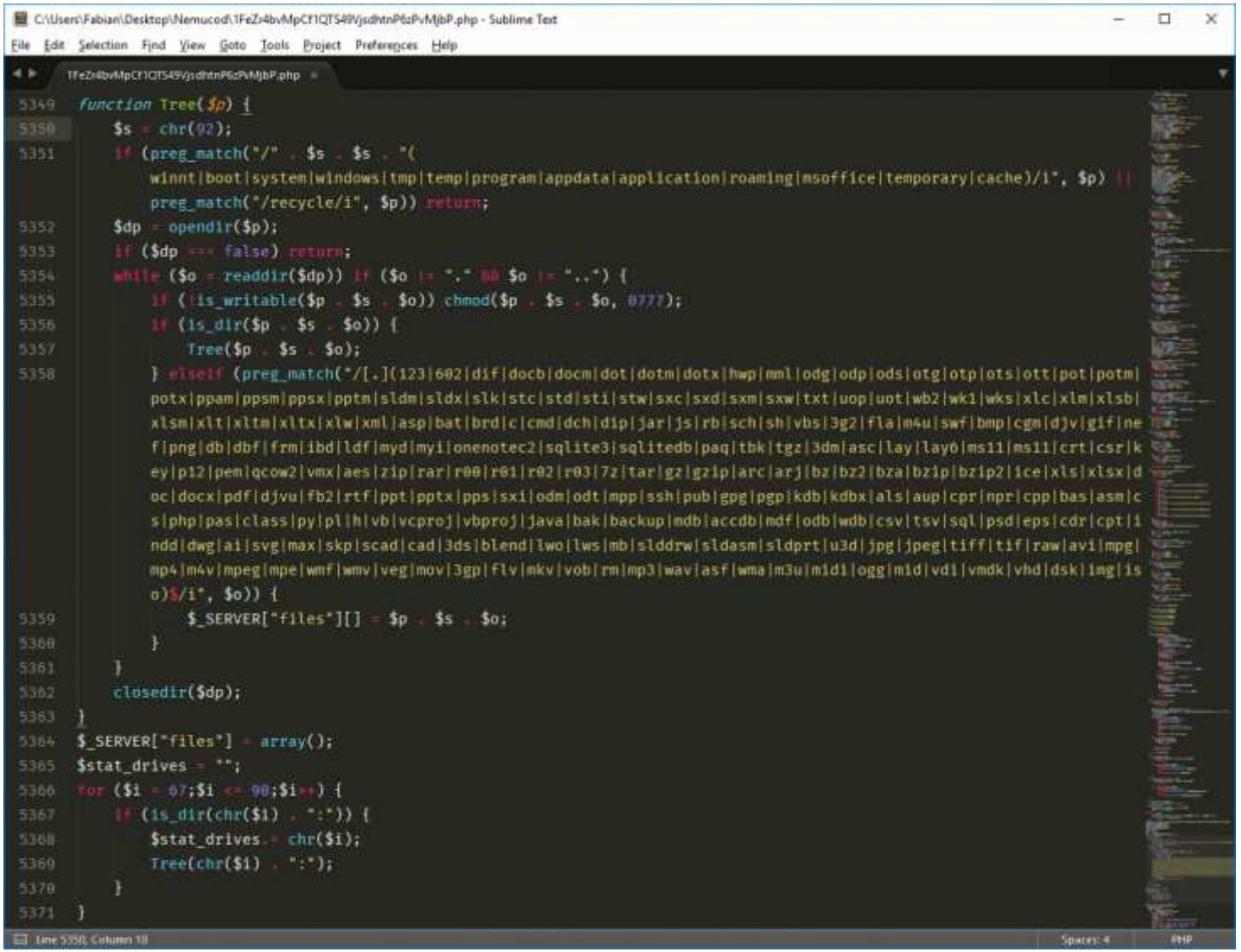


Source code of the JavaScript file that arrives at the victim

Once unsuspecting victims are fooled into running the script, the malware will download its ransomware component as well as the Kovter malware into the %TEMP% folder and where it executes both.

The NemucodAES ransomware component, which consists of a PHP script and the PHP interpreter, uses the same methods as previous variants to achieve persistence (read more about what ransomware does once it's on a computer here). Once the interpreter executes the script, it will then start cycling through all possible drive letters (including external and network drives) and starts the encryption process.

The key difference to previous members of this family is that the encryption has changed from RC4 to a mix of AES-128 in ECB mode and RSA encryption, an infamous combination that we explained in more detail in a recent blog post. In addition, it will not change any file extensions; so victims will only be aware of the damage done once they look at the garbled contents or cryptic error message when trying to open one of their documents.



Snippet of the code used to enumerates all drives for files to encrypt

NemucodAES ransomware targets the following file extensions:

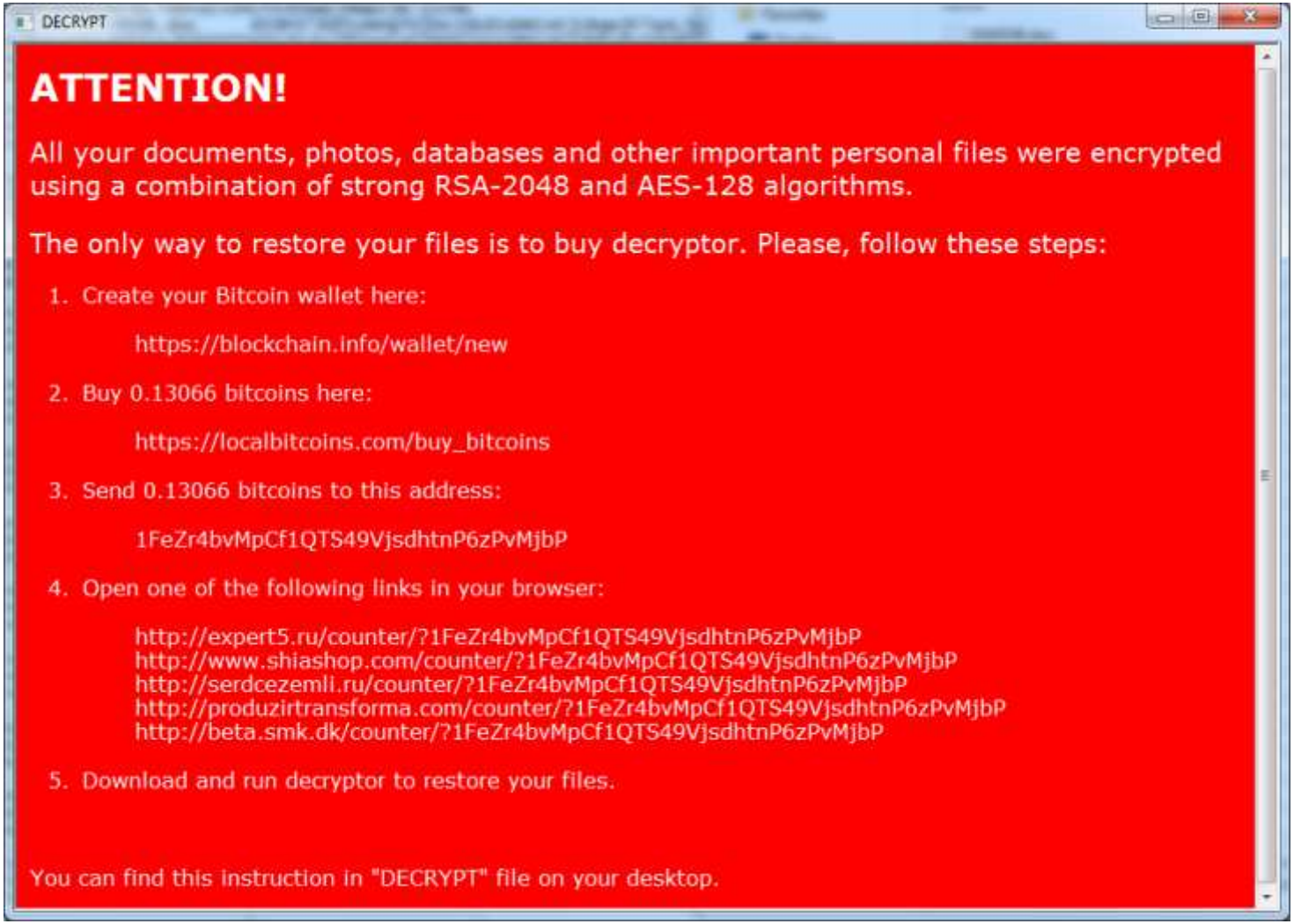
> .123, .602, .dif, .docb, .docm, .dot, .dotm, .dotx, .hwp, .mml, .odg, .odp, .ods, .otg, .otp, .ots, .ott, .pot, .potm, .potx, .ppam, .ppsm, .ppsx, .pptm, .sldm, .sldx, .slk, .stc, .std, .sti, .stw, .sxc, .sxd, .sxm, .sxw, .txt, .uop, .uot, .wb2, .wk1, .wks, .xlc, .xlm, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw, .xml, .asp, .bat, .brd, .c, .cmd, .dch, .dip, .jar, .js, .rb, .sch, .sh, .vbs, .3g2, .fla, .m4u, .swf, .bmp, .cgm, .djv, .gif, .nef, .png, .db, .dbf, .frm, .ibd, .ldf, .myd, .myi, .onenotec2, .sqlite3, .sqlitedb, .paq, .tbk, .tgz, .3dm, .asc, .lay, .lay6, .ms11, .ms11, .crt, .csr, .key, .p12, .pem, .qcow2, .vmx, .aes, .zip, .rar, .r00, .r01, .r02, .r03, .7z, .tar, .gz, .gzip, .arc, .arj, .bz, .bz2, .bza, .bzip, .bzip2, .ice, .xls, .xlsx, .doc, .docx, .pdf, .djvu, .fb2, .rtf, .ppt, .pptx, .pps, .sxi, .odm, .odt, .mpp, .ssh, .pub, .gpg, .pgp, .kdb, .kdbx, .als, .aup, .cpr, .npr, .cpp, .bas, .asm, .cs, .php, .pas, .class, .py, .pl, .h, .vb, .vcproj, .vbproj, .java, .bak, .backup, .mdb, .accdb, .mdf, .odb, .wdb, .csv, .tsv, .sql, .psd, .eps, .cdr, .cpt, .indd, .dwg, .ai, .svg, .max, .skp, .scad, .cad, .3ds, .blend, .lwo, .lws, .mb, .slddrw, .sldasm, .sldprt, .u3d, .jpg, .jpeg, .tiff, .tif, .raw, .avi, .mpg, .mp4, .m4v, .mpeg, .mpe, .wmf, .wmv, .veg, .mov, .3gp, .flv, .mkv, .vob, .rm, .mp3, .wav, .asf, .wma, .m3u, .midi, .ogg, .mid, .vdi, .vmdk, .vhd, .dsk, .img, .iso

In order to keep the system operational and ensure that folders critical to the functioning of the ransomware and later decryption remain intact, it will skip folders containing the following strings:

> \winnt, \boot, \system, \windows, \tmp, \temp, \program,\appdata, \application, \roaming, \msoffice, \temporary, \cache, recycler

Like its predecessors, NemucodAES only encrypts the first 2 KB of every targeted file. Unlike its predecessors, however, NemucodAES uses AES encryption with a randomly generated 128-bit per-file key. The encrypted data, as well as the file name and the RSA-encrypted AES keys, are then stored within a .db database file inside the %TEMP% directory. NemucodAES then overwrites the original first 2 KB of the file with random data.

Since the encrypted data is not stored within the files but within a separate database file, the file is essential for the decryption process as explained further down.

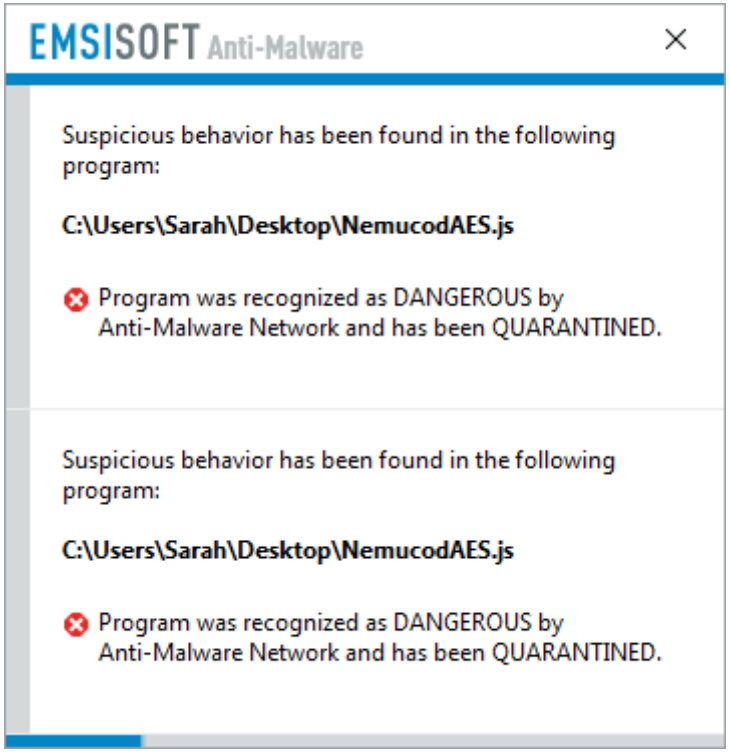


The NemucodAES ransom note left behind on the system

Last but not least the ransomware will delete any shadow copies stored on the system and create a ransom note on the victim's desktop named "DECRYPT.hta", instructing the victim to pay the equivalent of US $300 in Bitcoin to get back their files.

Are Emsisoft users protected?

Short answer: Yes! Our award winning Behavior Blocker technology with Anti-Ransomware layer has been able to stop NemucodAES dead in its tracks without the need for updates:



NemucodAES is no match for our behaviour blocker

If you want to see Emsisoft's Behavior Blocker in action against a wide variety of ransomware, check out our demonstration on YouTube.

For all non-Emsisoft customers: Decrypt your files using our free decrypter

Unfortunately, not everyone is enjoying the state-of-the-art protection Emsisoft products provide and we have seen an increase of victims hitting communities like BleepingComputer and ID Ransomware looking for help. For those victims, our lab created a special decrypter application that is able to restore affected files for free.

As explained in our thorough ransomware removal guide, it's critical to follow the right steps when dealing with and removing ransomware. We suggest to read it before attempting any hasty removal attempts. Particularly in this case, as any decrypter needs access to the database file within the %TEMP% folder that the

ransomware created in order to restore the files.

Many popular cleaning and optimizer programs, such as the popular CCleaner, delete files in the temp folder automatically, making the decryption process impossible for both the ransomware author's as well as our decrypter. So deactivate any such programs immediately and resist the temptation to blindly start cleaning.

Victims of NemucodAES ransomware can download our decrypter on our dedicated decrypter download page.

Have a great (ransomware-free) day!

www.emsisoft.com