Cryptbot downloader: A deep cryptanalysis - TEHTRIS

By Pierre-Henri PEZIER

Published: 2024-11-18 · Archived: 2026-04-05 18:46:14 UTC

Cryptbot is an advanced malware tool used in cyber-attacks, primarily targeting credentials, personal data, and cryptocurrency wallets. It functions as a stealer malware, capturing sensitive information like login credentials, browser cookies, and cryptocurrency wallet data. Distributed often through cracked software or malicious links, Cryptbot installs itself on victim devices without detection and begins data exfiltration. The stolen information is then sent to the attacker, potentially leading to identity theft or financial loss. Cryptbot is known for its rapid updates, making it difficult to detect and counter.

Among the numerous updates related to Cryptbot, its droppers have also evolved rapidly. A new variant featuring enhanced cryptography was recently released, with its command-and-control (C2) infrastructure remaining active for an extended period.

The main objectives of this article are to thoroughly understand the obfuscation mechanisms and to develop an automated exfiltration script.

Attack timeline

Based on the PE compilation timestamps found in each sample’s PE header, the active attack timeline has been mapped out and visualized in the following heatmap. The attack appears to have been conducted over a one-month span, with activity peaking approximately one week after the campaign began.

Based on the first submissions to VT (VirusTotal), we constructed a heatmap of the targeted victims. However, it is important to note that the submitter may not always be the actual target, so this data should be interpreted with caution. Russia appears to be the primary targeted country in this campaign.

Code detail

Code detail

The samples were developed using a compiler with the following flags: `-m32 -Wa,--noexecstack -Qunused-arguments -O3 -fPIC --static`. These flags indicate 32-bit architecture, a non-executable stack (`--noexecstack`), optimized code generation (`-O3`), position-independent code (`-fPIC`), and static linking (`--static`).

The libraries `libcurl 8.10.1` and `OpenSSL 3.3.2 (3 Sep 2024)` have been statically included in the sample. The obfuscator used to scramble the software's data flow remains unidentified.

Defense

The downloader includes defenses against reverse engineering and automated string extraction.

Data flow

The URLs of the C2 servers are stored in plaintext. To hinder automatic extraction, the last 6 to 8 bytes of each URL are append to the URL, making the string difficult to extract statically. This mechanism is the only method of data obfuscation used in the program. A custom script has been developed to reconstruct these URLs, included in the appendices. Due to the code's susceptibility to modifications caused by compiler optimization, an alternative *easter egg* hunting technique was applied. This script is provided in the appendices.

Control flow

nly the main function, which is responsible for calling the curl API, decrypting, and loading the DLL, has its control flow obfuscated. As shown in the capture below, the code is obfuscated using an extensive switch-case structure. However, due to the code’s relatively small size, it provides only limited resistance to reverse engineering through dynamic analysis.

Stealth

The sample was developed with debugging features enabled. Since it is compiled as a GUI application, adjusting the PE header to enable CLI functionality will cause a console window to appear, displaying debug messages.

Command and control

Identification

The full list of URLs is provided in the IOC (Indicators of Compromise) chapter. All identified C2 servers use a `.top` top-level domain (TLD).

Network

Protocols

The downloader retrieves the payload over unencrypted HTTP. Although the payload itself is encrypted, the headers and URL character set provide enough information to detect it using the Snort rule shown below.

Interestingly, the server provides a filename in the response header that does not match the URL of the GET request. This filename is later used to decrypt the payload.

Cryptography

The only cryptographic operation in the malware is performed on the data returned by the server. Although the data is transmitted over an unencrypted HTTP channel (which is very common with other malware families such as daolpu), the server response is encrypted, making it indistinguishable from random data.

The data returned by the server is AES-CBC encrypted, with the encryption key derived using PBKDF2-SHA1. The accompanying image illustrates the raw server response, where:

Blue portion: Encrypted ciphertext.

Red portion: PBKDF2-derived Initialization Vector (IV).

Green portion: AES-CBC Initialization Vector (IV).

The decryption routine in the Downloader has been fully reversed, as shown in the capture below. The process begins with key derivation, followed by decryption.

The key itself is a combination of the “filename” field returned in the HTTP header, the URL, and a string that is contained in the sample. This key generation process, derived from multiple sources, necessitates the following cleartext secrets to decrypt the stage2 payload:

- The ciphered data, obviously.
- The response header from the server.

- The sample URL.
- A static key suffix embedded within the sample.

This is a clever technique to make decryption of stage2 payloads impossible with only the network capture. Additionally, the 100,000 PBKDF2 rounds are specifically designed to make brute-forcing the key impractical.

To calculate the time required to decrypt the payload using only the network capture, we can use a simplified SHA-1 calculation as a reference. Since PBKDF2 applies 100,000 iterations, the time needed for brute-forcing would be approximately 100,000 times longer than a simple SHA-1 hash calculation (credit: proxynova.com).

A script has been developed to download the stage2 payload from the sample and gather all the necessary key components to perform the decryption. The following screenshot provides a preview of the script in action.

When the sample is deciphered, the DLL is manually loaded, as shown in the screenshot below. Despite the control flow scrambling, the MZ and PE header magic values are clearly identifiable, confirming the presence of a valid executable file format.

The SHA256 hashes of the Stage2 payloads are included in the IOC (Indicators of Compromise) section. The C2 servers are frequently shut down, making them unavailable at the time of writing. Additionally, the DLL is obfuscated, and further analysis or reverse engineering of this sample may be included in a future publication.

IOC

URLs

- http://home.eightji8ht.top/KTGbGvOSGlkPaQeuKdDL1572982449
- http://home.eightjo8sr.top/aCrmSMJLJEOsinOjzktg1889307302
- http://home.eightjo8vt.top/APWuDeoyrwjlLWFqpzlR1427917304
- http://home.eightjo8vt.top/GZAiWBsUWZXSjptiVgki1273022183
- http://home.eightjp8ht.top/FlchnxzGeSIHRPHPeYBm1318897305
- http://home.eightjp8vs.top/GyoNxLolJLOIDEEeLXwl1239497306
- http://home.eightjp8vs.top/feCIlgpoToBMdGHZfMGS1673054910
- http://home.eleja11sb.top/sSWxMfiKsjZhqgwqlqVX1737823123
- http://home.elevji11ht.top/XmQBHJYvyxRHnDxzxNoj124497298
- http://home.fiveji5ht.top/KlekgDAXLoeekVhmYBHz1732002979
- http://home.fiveji5ht.top/daxtYswdSfyAXDsFwHuK1726572986
- http://home.fiveji5ht.top/sYxNRoYrKJVZJBDMKRQb1729750322
- http://home.fiveji5vs.top/nGdZCFwukcqnsrEfVnqT1732922995
- http://home.fiveji5vt.top/NEpdjvSGIHCSlQWulCHt1776642968
- http://home.fivejo5sr.top/JNzvTWFWHwIXwNBdDJiw1743043030
- http://home.fivejo5sr.top/bTMlLHJsULflKiuhSKNo1745983026
- http://home.fivejo5vt.top/WTAjeFpNiEIhCJndAXAf1714163020
- http://home.fivejo5vt.top/bLeFEuIyIOOFgvRzlwsw1730462437
- http://home.fivejo5vt.top/jQDBoCTTJMoxHduEQtVi1718333022
- http://home.fivejo5vt.top/zViguzTHOAJchzMFSLOa1730123672
- http://home.fivejp5vs.top/WMIfiIbwGZlEzunsPmAm1791043054
- http://home.fivejp5vs.top/gEHGWhRNbwRFXwunSKCi1794913063
- http://home.fivjp5vt.top/GpXJRdeQulqmvESjfFlL1730790181
- http://home.fivjp5vt.top/MzxdLTzahBhrwcHfikEE1730826262
- http://home.forjh4ht.top/wGcuvRVzmafViJJtVGWe1729706625
- http://home.forji14vs.top/SRmkbXbtICjnsFSsyIIU1719933008
- http://home.forji14vs.top/vLzEmBxYDkDWwAHlJbwm1756532992
- http://home.forjo14vt.top/vZEhEBivXldclXHuMstz1714163020
- http://home.forpz4ht.top/cQOBChluQKBYyXAKOlUj1729771262
- http://home.neinja9ht.top/LQEGldMWvlStBQQIEVyV1797523097
- http://home.neinja9ht.top/xplvzowOfiYMuqANrGoq1730957812
- http://home.neinjo9vt.top/TCEdaQJXYbawpvRtmzAl1724603017
- http://home.neinjo9vt.top/fcOoKJiqkEdEfaSKlDpf1730221830
- http://home.neinjp9sr.top/VQZWuwklsiAqwKSHENhk1730865247
- http://home.ninjo19vs.top/kbrGrXsSXkmNPHYxWled1730607975
- http://home.oneji1vt.top/yYwXoctNQsNlxniaRRXW1729687663
- http://home.onejo1vs.top/VlQbIzlsEdAqLBFZBoYY1734910639
- http://home.onejo1vs.top/rwucRRJvgOJMYBxNQZTH1731060549
- http://home.onejo1vt.top/TgyonuAhQqHmRNCTtLXO1730221831
- http://home.onejo1vt.top/VBkFCJscNZobpQzbgGkx1736750123
- http://home.onejo1vt.top/pgpVedqwyWTKdnDvLton1739150427
- http://home.onejp1ht.top/EydgSnlRvnipiEFgnals1733640997
- http://home.onejp1ht.top/wjfslbMBCTjPKLMdHjMB1739381071
- http://home.onejp1vt.top/WVWXLEBFUCjXpjDFcYnq1730826262
- http://home.sevja17sb.top/LMiwiyYekyuSDTCvLbPv1765833112
- http://home.sevja17sb.top/ZsSuJntZcwEFCFkTKSrm1784413120
- http://home.sevjoi17ht.top/RZveVhltLlnLSesEiEKb1573051889
- http://home.sevjoi17sr.top/TCQEoezkVqyvrJjqBhZs1204307303
- http://home.sevjoi17vt.top/FhmmyqGhAphHaXwiJfvm1273042791
- http://home.sevjoi17vt.top/cZQSdrLXfSobDdFnqveX1701417302
- http://home.sevjp17vt.top/UDnaUWBbCguivjcJTAFI1730790183
- http://home.sevtji17vt.top/AtMFEEDPmrFgjjlYWVjB1487667296
- http://home.sivji6ht.top/nQOeaKPXEODJmfbxNDgw1726939767
- http://home.sivjo6vt.top/NkVbPqNMrXCEggsfRWGb1734600172
- http://home.sivjo6vt.top/RLcrqDvFJmGzdgZTXBGX1734380462
- http://home.sivjo6vt.top/ltLNFctqJMohaGeCvuMv1738320221
- http://home.sivjp6ht.top/lBxeEWboCtkXsZBdYMeP1738950518
- http://home.sixjp6sr.top/jtrLzFxhLfniIyrmfEOG1737810904
- http://home.sixtlm16ht.top/nbGcgYkZqJUuAbjyAxww1567697297
- http://home.sixtlm16sr.top/TGHTqHPiFFfksEXbQHwc1509887296

- http://home.tenja10ht.top/IGVMsWdjbQifeqDGdLik1778133095
- http://home.tenji10ht.top/MVPXmuUIFAQLfQdTpqGi1776942976
- http://home.tenjo10ht.top/FXpkGDyUTRqQxEvMSiPD1764033034
- http://home.tenjo10vt.top/paKURpJFxJCnukXyqZrN1779133042
- http://home.tenjp10vs.top/SFyYktVKDQBaqLympWfA1794923063
- http://home.thirtji13ht.top/MwOBqdodAGbyXMofAyrU5986261729
- http://home.thirtjo13sr.top/bYcMGmpHJcbGkomonWsU0126461730
- http://home.thirtjo13vt.top/FMmMtBkQtjnpYGvmAcfX3322181730
- http://home.thirtjo13vt.top/rvAMJqturkAmDaZoTnSo7412361730
- http://home.thirtjo13vt.top/xaDSPDgkqKmDlPNoQLbs1617302014
- http://home.tventji20ht.top/axNhXgnGYoPSgajZFkaQ5917298626
- http://home.tventji20vs.top/NWYJPzCYEvZpxoyKvBIK9295321729
- http://home.tventjo20sr.top/pLDNcrnQYnSceQqdUDvf0117302646
- http://home.tventjo20vs.top/SOMOJyZWYBxdybbmZeaW1270101730
- http://home.tventjo20vs.top/lwRwtEGztSQcWvXoArFS9063941730
- http://home.tventjo20vt.top/FjnNAcVhtuMKyKxfgwGc3022181730
- http://home.tventjo20vt.top/fExmNYmMwsMkeOPpBLzG1620141730
- http://home.tventjo20vt.top/ztcbHfsrgDVbKwvjMmcq7417301236
- http://home.tventjp20vt.top/julfUeXzXwHcgsxxhkmr6282621730
- http://home.twelja12sb.top/JLEncoVUzpBxNKNLrTYV1908437312
- http://home.twelja12sb.top/xKCOYZtRPmSqQvpgghZS1526587311
- http://home.twelji12ht.top/OsLGYXbzmZdjCMhTnuGb1972979319
- http://home.twelji12ht.top/VqfNYMmqQHyFNagmJCit1767697297
- http://home.twelji12ht.top/wUjNbZBIqtyGhfPTmpke1862657298
- http://home.twelji12vs.top/YKVZcYkIJkgPraRfOHBr1173008199
- http://home.twelji12vs.top/flyGQWUPyIQmXYOpcFMz1866977299
- http://home.twelji12vs.top/nXZUoCnprUWelKqFYScP1053297299
- http://home.tweljo12ht.top/SHfUuTYBULkoesjZJfWj1573051889
- http://home.tweljo12sr.top/AoVYhzVxzHmClkVkBHzK1964597302
- http://home.tweljo12sr.top/GDHlEMZKhUWZBxtHkRwh1573028930
- http://home.tweljo12sr.top/UPMCpUyoKEyLghAHklgZ1473030430
- http://home.tweljo12vs.top/GGjrrjEDEWQrYYIQCiSz1549107305
- http://home.tweljo12vs.top/awDRkLatDdHoLFjLkaTk1173065362
- http://home.tweljo12vt.top/GEZFdXtInPnroqnCxvvX1223677301
- http://home.tweljo12vt.top/OSVrAwHTMqXZwPLPhTMW1773013581
- http://home.tweljo12vt.top/UrZpabYUoOYCIETTggQp1273022183
- http://home.tweljp12ht.top/HoQpbeizPhmxJmnjugER1397367309
- http://home.tweljp12ht.top/QPoNBSMGOKYXiKKSXopP1257817309
- http://home.tweljp12ht.top/gwWsuyjcKfHgnGByabIj1771937310
- http://home.tweljp12ht.top/nQVpoVTlTakzyXMzpriM1279757309
- http://home.tweljp12vt.top/TLkmyWUrcoKSfuQMaKSm1173082626
- http://home.tweljp12vt.top/VszWEchGCZleshrQkPDo1986927307

Sample files

The SHA-256 list of downloader samples used in this article is as follows:

- 001ba21803795a450eac7e26fd14a1ae2ef32a5bad5e30b4dd765aad0e5ce7fe
- 01eff957b996465538f0e6a79791b1e7e551c2cb2d0e5c259bdc4ae3b13f48d6
- 02c7c64a8e5e65f6cd16f32bb9b1a4ac975b7479ffff638a2bb085b13825cab5
- 03e37248166df72e91aeb9640513d5a53ec449da4441af43263b447dbd38408b
- 051084d7828f88b80d0ae27fdd3c4baebba7fc82a916f8e7ce6376daf548cc20
- 08be4b7219442aadc19810463457dbd7bab6699f4de6e4dc00617d3429bd5b8c
- 0ad7e833d526131900916008913dec998360ee6d1a9aacf3997602e1cfc1c3e3
- 0f0c0fd81a7f69e33f27f920d639b4aa79c13a74f49231a756f41c3e94f206ab
- 1038bd204447881ed29e44f2288512d14745ad4a9acb1f9c26fbf388f002f9b8
- 12fa7b47d20f0f21ffeb0981eec1d017f377c9539a4d3ad3fca57897c6f5dfdf
- 14fcb1e15c8aae420a36ca53373b062b388605409cf3823642f217643126f07c
- 15b29945c813d2270d4a690719f319e79cda70c1cec2081cba3f05e80b3a549f
- 166421573e82a6a9ba03c7d10167bdb209fd4197305a719ab78b4c2918d69084
- 175957c7b7548858c963338e402325ae2bb249f7cd08d23c3e373b32a68d3b19
- 18b9b073f44dc79731988397997f8875aaf0025f17f89300ca16205b17c0ea35
- 199c28e2ac8b8cf866190c0733c9c010815b86e1eb842f3a9cfa43a73e05491d
- 1d346dcbb0a210552c6da5b8fe300c872b04b8aab052803baeb9f99d9062ad72

- 1f14b8a84d6052e40f434e310716c6a19b5604e194fb3a220d6f156a0cf4a7ff
- 23e7abfa4bbbaf8a8ff8afe139dd1874c4d1aba4826fc462da718ea2147c8c95
- 25e4f9e539d7e0461c55d4b4fa178c1cbb06760139e360da65648d777f118ca0
- 27b7915bbef99f765bee8aaa35f232a488c63138e7c0941da9a27d0057c92af6
- 2b1f016f12fef7124ea7c9898622e650e53814f2d5ff4d76fa712c3e591f9a7f
- 2bf5e06148f88f0ac9a1a33c9fc5b63b7ce65272fa4a234360600732df185007
- 30999b396ce17abf02b7bfb537222186a87c1554a1b9521bfb39dbee45a30288
- 30f0d55b444e180378dfa467bf13b5067b8faba7bc950b4765bb7dbc44ce3ce4
- 32eefa7f0b2893364c0de189b0c8a509ade84a07a463d6a1802c218f0dbb5817
- 332c1b9ad302388edf687fa6a4d8d5ca59dc609aac9215f8d5d8e659af6c615b
- 340d2dc26004646c86973f257b27d0d79491b652b02cc97f9149538cc2b65691
- 362f40028c50b3f13ea8e3ad2096e94ae325a53306d71263e4468101addf765e
- 3668b6e8b80edd909860784c326609470a1655c029dc797dbdceea92a81c83b2
- 3a378046ce52ea095ce8c5ec6aacabb98d73034fbe208dd298cdc75ad3dcfe8e
- 3accb1c82e64cdfce5d0aacd0093f71727575db426f75b77b6c98869c478ec27
- 465a1cefe61446110cc521d376651a5074fb87295da5fd64bd74fd25cbab669b
- 46c168c3108b54ca7f1495182e64b34b4470e8d383781a83a693ec6e6a7725ff
- 4b53e0fdcd937d34cf27f9938a30b977c1f64b5c954e1dc3225aaf4e7ce908ce
- 4b81371832a31aa1b9a3f4caf3da072dbadc9793dc92d90ba3ea89c8ba7dd17e
- 4cd6901726e36bcb39b33343f44a2facb79cfc8bee33e236ff2f603c01bd21a2
- 4ea653d806dd43b18c85cb0642fdaa92028e04864878c8ecb5c08cbe6eb98d61
- 5059ef43cacdc5bb03eb52112084059b3fa3c9f75179e52a9e8814f3c91e6a7f
- 51032e46bebfd6ed04fcc938f5cde48f26df6a0ec48d2b58d31e748c2d87222f
- 53b55b87c5329665f417c43fa8b44e7054183ab13714fd575f4ec73c1576d8d7
- 5ba2ca4455a95b2260a81b6e857735aa697146720db7d15508b69583feb4587d
- 5ea5c9b7b4b7f23b114533a39414f1eac9e6bfd4c1b87786c3840d1f7b6cdf0d
- 5f8d854a6883175c03086c4dfc5d9c8c797facbff6598b41b837f0945d8f1d1c
- 60003b32e48d426f486a0763229dc589ba64a4ca12adfe061732b3497df0930d
- 6008dc1e6448d5f98981eceeb428f0f8eb5ca5d01315073e7751f6812e64b887
- 606df073790843307f1e2cd1455b947a933def47e8a57b7df62f4a0d5e52a26b
- 61a6d4566575e72452bd3304822330f9d2f72accc4dbba11be4748618101fd63
- 6496ed3876803016bf5fb2018c13d9b4f2a7c44253774ebc7c7c36c0e5df7852
- 65841cfa9f5436f51683d7c359e8f2db9dd66723e6c875c6f5fc67d7b1358689
- 6813d84987f1ac92fb6b5d7a9f8ddf26424f44a55022cf9fc5563362c225d8b8
- 690d584a6a58a1e051ab1c0d3c92a3ebbd756125005be6b9ca31c870e801ce90
- 6a0120bf645d3c65aaadf28db313647e773da4d8be6d440f95e3ef3e020f95ce
- 6cb9ea7e7b8f9642e1effb00c75397dbcfe04291c3c61b1561786e46773f3fc2
- 724f947ba0d0b93369f1df6a55fe722889adff5a6f5922d7ab35389feeed13e6
- 73befffc90b6411e42b25b92b4860c8142c82232ff0fb8c247597d0bc09efdbd
- 75328c047ffd60f0ef0f461e8efd11b33f296b8229b9917846ee0a10679a3108
- 76273d86538a5a5ead5ffdae2fcad8d29ae93d736b1f3df1475da71c6a328c7b
- 7ce85df273257bb57c122c1bdceeebe59c16bd8629eff5ad494fb8c387ed7c8a
- 8003fd73d5681b78365343e95c96bf7289fbb66ad2e22673099f4ab4e947270f
- 80c8797268cb88f5bef1791ccc88b62288763a27528709886e55175b9bd94487
- 8350cb907603e05218052fde1fda489957f768aa49dc6ff122a6471d42101aaf
- 862331ec037b258171f1d9a5ff7ba0dd92cc82fab9c130513e4bab50821184e3
- 8682c6f437d339cb9b438cd76f93766dba9ff7db8e9b6ed5103e52d16e93f51f
- 895d6d80e1b7b5ae2745bd7c7d29c9ad3740a4aea90e3ee5035f60ae91ed7c18
- 8af6d1cf38790da6c8205c4cfa20d43e79aebde03571bd881379d1fbbf13f07b
- 8c209705b91becbc186f2aafd2b8dbdffe1b78f0c765ff4d62e9fd7be52c926a
- 8c81a5f325bacafc6094e8d31881ff27de9ecdbcd1c20d67f1e298be09be2ee7
- 8f9fb0dbcf09f7b0a2838323c55a4cb3ce5ebd29230b9afc65cc6e23eb57d107
- 91c3092bc46c0b23b39d0cc10ddeee1b0008d0a12aed25791ed322ef7bc10792
- 9415e13f69bce584aa0e94ba833d689f892d27960f6b6b353f439e4aee32b1aa
- 983d11c7f6d115e3938ebc92b1ade92ea247c44632b3330af256693c2641cb99
- 9b827d471a9e2bd4249aa1cfb80721b97316334fd5aecbc5e2d4296e1c088a12
- 9c45c5456167f65156faa1313ad8bbaffb8aa375669bf756fe0273580a621494
- 9e8de744db5b8cd794226a4df549804f2dcd0f235d035e89305ca093dc3936c2
- a175dbaa581c7064effea9150163c84d5e6e12f975103c31dc13caeb85b62e47
- a2490d03cf08a0cc48030c915a1d6f17a7f755edf84f825df7ae752a358d8837
- a442c37a225f1417da4e67d87d44eb95cb90198f146f09fc4d2da1f716866866
- a55616e2551ae292c035fdb2ceba08327464394e6ec115c424f0e4340a50634d
- a725a1282151b3d66b12e29c116980c7837ae3829682914cf920e0b4520808e7
- aa7c16c9b06e1bc8012e1865a3fa18dd8f43b56c133649fb7ef25400fecea920

- ac94431fdba78b69ba481a37c56e4d067eb26844b64603e946ac402ef344ba4d
- b4222cd9bfbe897a10395414da0f744e223aba7c3ffeee68f03dbd167835c3cb
- b6e865ee7366584424eee3c120bfa7e510fdd1ddd85bd6e59aef57546be13dbd
- b7439cb886010a0f42601044ff3b1ff2cd11873a6e16b6682cba31e052f5865d
- bc417517a6b5949226151ed2dc3b398051fabe68c7c1b1ad92279e6425761962
- bd309518a3159b042d5f766c6159afbad5b18d8c6058d3a20773899a18314b21
- bdd3db5c703b69a6e146f1475d611468ec92053cc25c1b8bd256a56ae1624eb0
- be232e6678efb17e42750a84a60d69ebe71b0bff28e028a375559499782a66b7
- c297513faa34104fe812a1e59d0f98fb6fe741d2ddb2fc424dce33ee175a8c7e
- c332f3148d35b98d5b9aebb25f7642bf2315476edf8640f4e49a04bff7ef1992
- c7049f22ae5ea4adfba9a137ee331874fee567dcfca6ef04cddbd520d7b00ece
- cafb2d43814edf00a88b69ef44a0cdd7f8217b05132638bfe62a633b021be963
- ce3b09833cb88e8dda668604a50dee535f3ab3f9edc258e2a2f389064065d1b9
- cf374b923e49a731b035faae8fb0756e71d8377dc4b584fc51595320b1e5bc23
- d132b6b606284363684e9ed72fa516c751c5a5447a7af78b803b368a68e1319b
- d441fadd2e5dfbf526802b611391a7433578c8b507757bd606f873dde76ba290
- d539ced1656cbeda5fb3c9fa7a7dd15d379543877921fb6b988fe1ff0e5cb65a
- d8a7d38189c1b552ba07b3c12536c9cb9f7291161180937c08d28c736e3a84bc
- dcc3e88eabf7700facf18c6f905d21c1450e38f17190d38afabfb5aede2d2aab
- de0461d80b3a5986cd7a290620f4e1096b86a80ecb72e5033af944a0a368e374
- dfdc63994c85f7161e25a26b762835781ce5578c6a5b5c2839324fc7faa591d3
- e0366f1f6d7d396f6ef06b8398f9d899c94757449ee32b45ff855d77d1442256
- e10a1bde9ed99785982416b20443e1c9387375876cf21887f6470f32d29eeac6
- e597f985a19237355dd489fa6eb95fdcb22b6d1a5125574aceb1c82e42057e72
- e5a9c5284062d9862dba21c860b32d6f58559175af193c052d0d968a17336d98
- f0f57933cba2b43988458cab4e386e4949902c23df723a97eb8da53bd8d4a49d
- f2c4f0c152acbb4a8e575e6095fc84b6df932e114c4f2a32a69d1ed19c1a55f7
- f4c3fecde4a9a5557fe1eca14b6b051aeb3c282780d51163ad4e11ef32454d20
- f89b07f4043c0bccd8537ed6a24f15932b9f70cc10743e022487bee62c075f98
- fa0aefa912e04ffcb1895e917d24372816c9da6f827b36079eaa115a0349dc0a
- faf630469655fcddb34a6bb2f24a5857bd36fd463760fe7643dbeb3f080b9a72
- fba6378aaf31225825c21cc7b06e1e8a408102bdba7a18a1b3d84b23cfe08018
- fbcf1356f2c11fe73efe69c1eba77a62ae742c935f3232dbed77657408a06933

Stage2 cryptbot files

The list of Stage2 Cryptbot payload DLLs used in this article includes the following:

- dfdc63994c85f7161e25a26b762835781ce5578c6a5b5c2839324fc7faa591d3.dll
- dfefcc62121ee76f84d382fc622b61321f149a04a848c8cb987a7bda7ca59941.dll

Detection

Yara

```
 import "pe"

rule test {
    meta:
        author = "PEZIER Pierre-Henri. Copyright TEHTRIS 2024"
    strings:
        $ossl = "openssl"
         $curl = "curl"
         $mingw32 = "mingw32"

        $s01 = "file_name is  %s" ascii fullword
        $s02 = "password len %d and %d" ascii fullword
        $s03 = "Memory allocation failed for passw1." ascii fullword
        $s04 = "Combined password:" ascii fullword
        $s05 = "Failed to load DLL from memory" ascii fullword
        $s06 = "after MemoryLoadLibrary" ascii fullword
        $s07 = "main" ascii fullword
        $s08 = "Failed to get the address of the exported function" ascii fullword
        $s09 = "after MemoryGetProcAddress" ascii fullword
        $s10 = "after exportedFunction" ascii fullword
        $s11 = "Hello, World!" ascii fullword
        $s12 = "Decrypted data: %s" ascii fullword
```

```
        $s13 = "Decryption failed." ascii fullword
        $s14 = "Failed to download the file." ascii fullword
    condition:
            pe.is_pe and $ossl and $curl and $mingw32
            and 5 of ($s*)
}
```

snort

```
alert http any any -> any any (\
   sid: 130000006;\
   metadata: author PEZIER Pierre-Henri. Copyright TEHTRIS 2024;\
   msg: "CryptBotDropper";\
   flow: established, to_server;\
   content:!"User-Agent|3A|";\
   content:"GET"; http_method;\
   http.uri; pcre: "/\/[a-z]{15,}[0-9]{8,}/i";\
   http.host; pcre: "/^home\.[a-z0-9]+\.top$/i";\
   rev: 1; )
```

Appendice

Stage2 download and decryption script

```
import pathlib
import magic
import sys
import re
import struct
from termcolor import colored
import hashlib
import requests
import click
import click_pathlib
from Crypto.Protocol.KDF import PBKDF2
from Crypto.Cipher import AES
from Crypto.Hash import SHA1
import yara
import os


YARA = yara.compile(source="""
import "pe"

rule test {
    strings:
        $ossl = "openssl"
        $curl = "curl"
        $mingw32 = "mingw32"

        $s01 = "file_name is  %s" ascii fullword
        $s02 = "password len %d and %d" ascii fullword
        $s03 = "Memory allocation failed for passw1." ascii fullword
        $s04 = "Combined password:" ascii fullword
        $s05 = "Failed to load DLL from memory" ascii fullword
        $s06 = "after MemoryLoadLibrary" ascii fullword
        $s07 = "main" ascii fullword
        $s08 = "Failed to get the address of the exported function" ascii fullword
        $s09 = "after MemoryGetProcAddress" ascii fullword
        $s10 = "after exportedFunction" ascii fullword
        $s11 = "Hello, World!" ascii fullword
        $s12 = "Decrypted data: %s" ascii fullword
        $s13 = "Decryption failed." ascii fullword
        $s14 = "Failed to download the file." ascii fullword
    condition:
        filesize < 10MB and pe.is_pe and $ossl and $curl and $mingw32
        and 5 of ($s*)
```

```
}
""")


def printok(string: str) -> None:
    print(colored(f"[+] {string}", "green"))

@click.command("download")
@click.argument("file_path", type=click_pathlib.Path(exists=True))
@click.argument("output", type=click_pathlib.Path(exists=False))
def download_stage2(file_path: pathlib.Path, output: pathlib.Path) -> None:
    printok(f"processing: {file_path}")
    file_data = file_path.read_bytes()
    # Check the file validity
    assert YARA.match(str(file_path)), "This file does not seems to be a compatible ownloader version"
    # Extract the URL and key from the file
    printok("Found downloader")
    assert (credentials := re.search(rb"(?ims)([@a-z\d]+)\x00+(http://.*?)(?=\x00)", file_data)), "Unable to find url and k
    assert (endurl := re.search(rb"(\xE8|\xBE|\xBA|\xBB)(?P<k1>\d{3,4}).{,128}(\xB8|\xBF|\xB9)(?P<k2>\d{3,4})", file_data))
    try:
        key = credentials.group(1).decode("UTF-8")
        url = credentials.group(2).decode("UTF-8")
    except UnicodeDecodeError as error:
        raise AssertionError("Unable to decode url and key") from error
    printok("Encryption key extracted successfully")
    # Perform download
    url = f'{url}{endurl.group("k1").decode("UTF-8")}{endurl.group("k2").decode("UTF-8")}'
    try:
        printok(f"Downloading: {url}")
        response = requests.get(url, headers={"User-Agent": ""})
    except (requests.exceptions.RequestException) as error:
        raise AssertionError("Unable to connect to the C2") from error
    assert response.status_code == 200, "Wrong response from C2"
    assert response.content, "Empty response from C2"
    assert (content_disposition := response.headers.get("Content-Disposition")) and re.search(r'filename="(.*);"', content_
    printok("Stage2 downloaded successfully")
    server_key = re.search(r'filename="(.*);"', content_disposition).group(1)
    # Decrypt and unpad
    combined_password = f"{key}{server_key}"[-36:]
    aes_key = PBKDF2(combined_password.encode("UTF-8"), response.content[:16], 32, count=100000, hmac_hash_module=SHA1)
    cleartext = AES.new(aes_key, AES.MODE_CBC, response.content[16:32]).decrypt(response.content[32:])
    cleartext = cleartext.rstrip(bytes((cleartext[-1],)) * cleartext[-1])
    # check the output
    assert magic.from_buffer(cleartext).startswith("PE"), "Not a valid PE file"
    output.write_bytes(cleartext)
    printok(f"File extracted to: {output.resolve()}")



if __name__ == "__main__":
    if os.name == "nt":
        os.system("color")
    try:
        download_stage2()
    except AssertionError as error:
        print(colored(f"[-] {error}", "red"), file=sys.stderr)
        sys.exit(1)
```

Misp formatted IOC

```
{
   "Event": {
       "info": "Cryptbot Malware Indicators",
       "date": "2024-11-15",
       "threat_level_id": 3,
       "attribute_count": 216,
       "attributes": [
           {
               "type": "sha256",
```

```
            "value": "001ba21803795a450eac7e26fd14a1ae2ef32a5bad5e30b4dd765aad0e5ce7fe",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "01eff957b996465538f0e6a79791b1e7e551c2cb2d0e5c259bdc4ae3b13f48d6",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "02c7c64a8e5e65f6cd16f32bb9b1a4ac975b7479ffff638a2bb085b13825cab5",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "03e37248166df72e91aeb9640513d5a53ec449da4441af43263b447dbd38408b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "051084d7828f88b80d0ae27fdd3c4baebba7fc82a916f8e7ce6376daf548cc20",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "08be4b7219442aadc19810463457dbd7bab6699f4de6e4dc00617d3429bd5b8c",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "0ad7e833d526131900916008913dec998360ee6d1a9aacf3997602e1cfc1c3e3",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "0f0c0fd81a7f69e33f27f920d639b4aa79c13a74f49231a756f41c3e94f206ab",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "1038bd204447881ed29e44f2288512d14745ad4a9acb1f9c26fbf388f002f9b8",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "12fa7b47d20f0f21ffeb0981eec1d017f377c9539a4d3ad3fca57897c6f5dfdf",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "14fcb1e15c8aae420a36ca53373b062b388605409cf3823642f217643126f07c",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "15b29945c813d2270d4a690719f319e79cda70c1cec2081cba3f05e80b3a549f",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
```

```
            "type": "sha256",
            "value": "166421573e82a6a9ba03c7d10167bdb209fd4197305a719ab78b4c2918d69084",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "175957c7b7548858c963338e402325ae2bb249f7cd08d23c3e373b32a68d3b19",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "18b9b073f44dc79731988397997f8875aaf0025f17f89300ca16205b17c0ea35",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "199c28e2ac8b8cf866190c0733c9c010815b86e1eb842f3a9cfa43a73e05491d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "1d346dcbb0a210552c6da5b8fe300c872b04b8aab052803baeb9f99d9062ad72",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "1f14b8a84d6052e40f434e310716c6a19b5604e194fb3a220d6f156a0cf4a7ff",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "23e7abfa4bbbaf8a8ff8afe139dd1874c4d1aba4826fc462da718ea2147c8c95",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "25e4f9e539d7e0461c55d4b4fa178c1cbb06760139e360da65648d777f118ca0",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "27b7915bbef99f765bee8aaa35f232a488c63138e7c0941da9a27d0057c92af6",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "2b1f016f12fef7124ea7c9898622e650e53814f2d5ff4d76fa712c3e591f9a7f",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "2bf5e06148f88f0ac9a1a33c9fc5b63b7ce65272fa4a234360600732df185007",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "30999b396ce17abf02b7bfb537222186a87c1554a1b9521bfb39dbee45a30288",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
```

```
        {
            "type": "sha256",
            "value": "30f0d55b444e180378dfa467bf13b5067b8faba7bc950b4765bb7dbc44ce3ce4",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "32eefa7f0b2893364c0de189b0c8a509ade84a07a463d6a1802c218f0dbb5817",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "332c1b9ad302388edf687fa6a4d8d5ca59dc609aac9215f8d5d8e659af6c615b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "340d2dc26004646c86973f257b27d0d79491b652b02cc97f9149538cc2b65691",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "362f40028c50b3f13ea8e3ad2096e94ae325a53306d71263e4468101addf765e",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "3668b6e8b80edd909860784c326609470a1655c029dc797dbdceea92a81c83b2",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "3a378046ce52ea095ce8c5ec6aacabb98d73034fbe208dd298cdc75ad3dcfe8e",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "3accb1c82e64cdfce5d0aacd0093f71727575db426f75b77b6c98869c478ec27",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "465a1cefe61446110cc521d376651a5074fb87295da5fd64bd74fd25cbab669b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "46c168c3108b54ca7f1495182e64b34b4470e8d383781a83a693ec6e6a7725ff",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "4b53e0fdcd937d34cf27f9938a30b977c1f64b5c954e1dc3225aaf4e7ce908ce",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "4b81371832a31aa1b9a3f4caf3da072dbadc9793dc92d90ba3ea89c8ba7dd17e",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
```

```
        },
        {
            "type": "sha256",
            "value": "4cd6901726e36bcb39b33343f44a2facb79cfc8bee33e236ff2f603c01bd21a2",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "4ea653d806dd43b18c85cb0642fdaa92028e04864878c8ecb5c08cbe6eb98d61",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "5059ef43cacdc5bb03eb52112084059b3fa3c9f75179e52a9e8814f3c91e6a7f",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "51032e46bebfd6ed04fcc938f5cde48f26df6a0ec48d2b58d31e748c2d87222f",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "53b55b87c5329665f417c43fa8b44e7054183ab13714fd575f4ec73c1576d8d7",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "5ba2ca4455a95b2260a81b6e857735aa697146720db7d15508b69583feb4587d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "5ea5c9b7b4b7f23b114533a39414f1eac9e6bfd4c1b87786c3840d1f7b6cdf0d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "5f8d854a6883175c03086c4dfc5d9c8c797facbff6598b41b837f0945d8f1d1c",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "60003b32e48d426f486a0763229dc589ba64a4ca12adfe061732b3497df0930d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "6008dc1e6448d5f98981eceeb428f0f8eb5ca5d01315073e7751f6812e64b887",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "606df073790843307f1e2cd1455b947a933def47e8a57b7df62f4a0d5e52a26b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "61a6d4566575e72452bd3304822330f9d2f72accc4dbba11be4748618101fd63",
            "category": "Payload delivery",
```

```
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "6496ed3876803016bf5fb2018c13d9b4f2a7c44253774ebc7c7c36c0e5df7852",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "65841cfa9f5436f51683d7c359e8f2db9dd66723e6c875c6f5fc67d7b1358689",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "6813d84987f1ac92fb6b5d7a9f8ddf26424f44a55022cf9fc5563362c225d8b8",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "690d584a6a58a1e051ab1c0d3c92a3ebbd756125005be6b9ca31c870e801ce90",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "6a0120bf645d3c65aaadf28db313647e773da4d8be6d440f95e3ef3e020f95ce",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "6cb9ea7e7b8f9642e1effb00c75397dbcfe04291c3c61b1561786e46773f3fc2",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "724f947ba0d0b93369f1df6a55fe722889adff5a6f5922d7ab35389feeed13e6",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "73befffc90b6411e42b25b92b4860c8142c82232ff0fb8c247597d0bc09efdbd",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "75328c047ffd60f0ef0f461e8efd11b33f296b8229b9917846ee0a10679a3108",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "76273d86538a5a5ead5ffdae2fcad8d29ae93d736b1f3df1475da71c6a328c7b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "7ce85df273257bb57c122c1bdceeebe59c16bd8629eff5ad494fb8c387ed7c8a",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8003fd73d5681b78365343e95c96bf7289fbb66ad2e22673099f4ab4e947270f",
```

```
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "80c8797268cb88f5bef1791ccc88b62288763a27528709886e55175b9bd94487",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8350cb907603e05218052fde1fda489957f768aa49dc6ff122a6471d42101aaf",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "862331ec037b258171f1d9a5ff7ba0dd92cc82fab9c130513e4bab50821184e3",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8682c6f437d339cb9b438cd76f93766dba9ff7db8e9b6ed5103e52d16e93f51f",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "895d6d80e1b7b5ae2745bd7c7d29c9ad3740a4aea90e3ee5035f60ae91ed7c18",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8af6d1cf38790da6c8205c4cfa20d43e79aebde03571bd881379d1fbbf13f07b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8c209705b91becbc186f2aafd2b8dbdffe1b78f0c765ff4d62e9fd7be52c926a",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8c81a5f325bacafc6094e8d31881ff27de9ecdbcd1c20d67f1e298be09be2ee7",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "8f9fb0dbcf09f7b0a2838323c55a4cb3ce5ebd29230b9afc65cc6e23eb57d107",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "91c3092bc46c0b23b39d0cc10ddeee1b0008d0a12aed25791ed322ef7bc10792",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "9415e13f69bce584aa0e94ba833d689f892d27960f6b6b353f439e4aee32b1aa",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
```

```
            "value": "983d11c7f6d115e3938ebc92b1ade92ea247c44632b3330af256693c2641cb99",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "9b827d471a9e2bd4249aa1cfb80721b97316334fd5aecbc5e2d4296e1c088a12",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "9c45c5456167f65156faa1313ad8bbaffb8aa375669bf756fe0273580a621494",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "9e8de744db5b8cd794226a4df549804f2dcd0f235d035e89305ca093dc3936c2",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "a175dbaa581c7064effea9150163c84d5e6e12f975103c31dc13caeb85b62e47",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "a2490d03cf08a0cc48030c915a1d6f17a7f755edf84f825df7ae752a358d8837",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "a442c37a225f1417da4e67d87d44eb95cb90198f146f09fc4d2da1f716866866",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "a55616e2551ae292c035fdb2ceba08327464394e6ec115c424f0e4340a50634d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "a725a1282151b3d66b12e29c116980c7837ae3829682914cf920e0b4520808e7",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "aa7c16c9b06e1bc8012e1865a3fa18dd8f43b56c133649fb7ef25400fecea920",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "ac94431fdba78b69ba481a37c56e4d067eb26844b64603e946ac402ef344ba4d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "b4222cd9bfbe897a10395414da0f744e223aba7c3ffeee68f03dbd167835c3cb",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
```

```
            "type": "sha256",
            "value": "b6e865ee7366584424eee3c120bfa7e510fdd1ddd85bd6e59aef57546be13dbd",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "b7439cb886010a0f42601044ff3b1ff2cd11873a6e16b6682cba31e052f5865d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "bc417517a6b5949226151ed2dc3b398051fabe68c7c1b1ad92279e6425761962",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "bd309518a3159b042d5f766c6159afbad5b18d8c6058d3a20773899a18314b21",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "bdd3db5c703b69a6e146f1475d611468ec92053cc25c1b8bd256a56ae1624eb0",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "be232e6678efb17e42750a84a60d69ebe71b0bff28e028a375559499782a66b7",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "c297513faa34104fe812a1e59d0f98fb6fe741d2ddb2fc424dce33ee175a8c7e",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "c332f3148d35b98d5b9aebb25f7642bf2315476edf8640f4e49a04bff7ef1992",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "c7049f22ae5ea4adfba9a137ee331874fee567dcfca6ef04cddbd520d7b00ece",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "cafb2d43814edf00a88b69ef44a0cdd7f8217b05132638bfe62a633b021be963",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "ce3b09833cb88e8dda668604a50dee535f3ab3f9edc258e2a2f389064065d1b9",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "cf374b923e49a731b035faae8fb0756e71d8377dc4b584fc51595320b1e5bc23",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
```

```
        {
            "type": "sha256",
            "value": "d132b6b606284363684e9ed72fa516c751c5a5447a7af78b803b368a68e1319b",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "d441fadd2e5dfbf526802b611391a7433578c8b507757bd606f873dde76ba290",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "d539ced1656cbeda5fb3c9fa7a7dd15d379543877921fb6b988fe1ff0e5cb65a",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "d8a7d38189c1b552ba07b3c12536c9cb9f7291161180937c08d28c736e3a84bc",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "dcc3e88eabf7700facf18c6f905d21c1450e38f17190d38afabfb5aede2d2aab",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "de0461d80b3a5986cd7a290620f4e1096b86a80ecb72e5033af944a0a368e374",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "dfdc63994c85f7161e25a26b762835781ce5578c6a5b5c2839324fc7faa591d3",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "e0366f1f6d7d396f6ef06b8398f9d899c94757449ee32b45ff855d77d1442256",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "e10a1bde9ed99785982416b20443e1c9387375876cf21887f6470f32d29eeac6",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "e597f985a19237355dd489fa6eb95fdcb22b6d1a5125574aceb1c82e42057e72",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "e5a9c5284062d9862dba21c860b32d6f58559175af193c052d0d968a17336d98",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "f0f57933cba2b43988458cab4e386e4949902c23df723a97eb8da53bd8d4a49d",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
```

```
        },
        {
            "type": "sha256",
            "value": "f2c4f0c152acbb4a8e575e6095fc84b6df932e114c4f2a32a69d1ed19c1a55f7",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "f4c3fecde4a9a5557fe1eca14b6b051aeb3c282780d51163ad4e11ef32454d20",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "f89b07f4043c0bccd8537ed6a24f15932b9f70cc10743e022487bee62c075f98",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "fa0aefa912e04ffcb1895e917d24372816c9da6f827b36079eaa115a0349dc0a",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "faf630469655fcddb34a6bb2f24a5857bd36fd463760fe7643dbeb3f080b9a72",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "fba6378aaf31225825c21cc7b06e1e8a408102bdba7a18a1b3d84b23cfe08018",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "sha256",
            "value": "fbcf1356f2c11fe73efe69c1eba77a62ae742c935f3232dbed77657408a06933",
            "category": "Payload delivery",
            "comment": "Cryptbot payload hash"
        },
        {
            "type": "url",
            "value": "* http://home.eightji8ht.top/KTGbGvOSGlkPaQeuKdDL1572982449",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjo8sr.top/aCrmSMJLJEOsinOjzktg1889307302",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjo8vt.top/APWuDeoyrwjlLWFqpzlR1427917304",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjo8vt.top/GZAiWBsUWZXSjptiVgki1273022183",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjp8ht.top/FlchnxzGeSIHRPHPeYBm1318897305",
            "category": "Network activity",
```

```
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjp8vs.top/GyoNxLolJLOIDEEeLXwl1239497306",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eightjp8vs.top/feCIlgpoToBMdGHZfMGS1673054910",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.eleja11sb.top/sSWxMfiKsjZhqgwqlqVX1737823123",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.elevji11ht.top/XmQBHJYvyxRHnDxzxNoj124497298",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fiveji5ht.top/KlekgDAXLoeekVhmYBHz1732002979",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fiveji5ht.top/daxtYswdSfyAXDsFwHuK1726572986",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fiveji5ht.top/sYxNRoYrKJVZJBDMKRQb1729750322",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fiveji5vs.top/nGdZCFwukcqnsrEfVnqT1732922995",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fiveji5vt.top/NEpdjvSGIHCSlQWulCHt1776642968",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5sr.top/JNzvTWFWHwIXwNBdDJiw1743043030",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5sr.top/bTMlLHJsULflKiuhSKNo1745983026",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5vt.top/WTAjeFpNiEIhCJndAXAf1714163020",
```

```
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5vt.top/bLeFEuIyIOOFgvRzlwsw1730462437",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5vt.top/jQDBoCTTJMoxHduEQtVi1718333022",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejo5vt.top/zViguzTHOAJchzMFSLOa1730123672",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejp5vs.top/WMIfiIbwGZlEzunsPmAm1791043054",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivejp5vs.top/gEHGWhRNbwRFXwunSKCi1794913063",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivjp5vt.top/GpXJRdeQulqmvESjfFlL1730790181",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.fivjp5vt.top/MzxdLTzahBhrwcHfikEE1730826262",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.forjh4ht.top/wGcuvRVzmafViJJtVGWe1729706625",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.forji14vs.top/SRmkbXbtICjnsFSsyIIU1719933008",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.forji14vs.top/vLzEmBxYDkDWwAHlJbwm1756532992",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.forjo14vt.top/vZEhEBivXldclXHuMstz1714163020",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
```

```
        "value": "* http://home.forpz4ht.top/cQOBChluQKBYyXAKOlUj1729771262",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.neinja9ht.top/LQEGldMWvlStBQQIEVyV1797523097",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.neinja9ht.top/xplvzowOfiYMuqANrGoq1730957812",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.neinjo9vt.top/TCEdaQJXYbawpvRtmzAl1724603017",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.neinjo9vt.top/fcOoKJiqkEdEfaSKlDpf1730221830",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.neinjp9sr.top/VQZWuwklsiAqwKSHENhk1730865247",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.ninjo19vs.top/kbrGrXsSXkmNPHYxWled1730607975",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.oneji1vt.top/yYwXoctNQsNlxniaRRXW1729687663",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.onejo1vs.top/VlQbIzlsEdAqLBFZBoYY1734910639",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.onejo1vs.top/rwucRRJvgOJMYBxNQZTH1731060549",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.onejo1vt.top/TgyonuAhQqHmRNCTtLXO1730221831",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
        "type": "url",
        "value": "* http://home.onejo1vt.top/VBkFCJscNZobpQzbgGkx1736750123",
        "category": "Network activity",
        "comment": "Cryptbot C2 URL"
    },
    {
```

```
            "type": "url",
            "value": "* http://home.onejo1vt.top/pgpVedqwyWTKdnDvLton1739150427",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.onejp1ht.top/EydgSnlRvnipiEFgnals1733640997",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.onejp1ht.top/wjfslbMBCTjPKLMdHjMB1739381071",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.onejp1vt.top/WVWXLEBFUCjXpjDFcYnq1730826262",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevja17sb.top/LMiwiyYekyuSDTCvLbPv1765833112",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevja17sb.top/ZsSuJntZcwEFCFkTKSrm1784413120",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevjoi17ht.top/RZveVhltLlnLSesEiEKb1573051889",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevjoi17sr.top/TCQEoezkVqyvrJjqBhZs1204307303",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevjoi17vt.top/FhmmyqGhAphHaXwiJfvm1273042791",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevjoi17vt.top/cZQSdrLXfSobDdFnqveX1701417302",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevjp17vt.top/UDnaUWBbCguivjcJTAFI1730790183",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sevtji17vt.top/AtMFEEDPmrFgjjlYWVjB1487667296",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
```

```
        {
            "type": "url",
            "value": "* http://home.sivji6ht.top/nQOeaKPXEODJmfbxNDgw1726939767",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sivjo6vt.top/NkVbPqNMrXCEggsfRWGb1734600172",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sivjo6vt.top/RLcrqDvFJmGzdgZTXBGX1734380462",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sivjo6vt.top/ltLNFctqJMohaGeCvuMv1738320221",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sivjp6ht.top/lBxeEWboCtkXsZBdYMeP1738950518",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sixjp6sr.top/jtrLzFxhLfniIyrmfEOG1737810904",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sixtlm16ht.top/nbGcgYkZqJUuAbjyAxww1567697297",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.sixtlm16sr.top/TGHTqHPiFFfksEXbQHwc1509887296",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tenja10ht.top/IGVMsWdjbQifeqDGdLik1778133095",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tenji10ht.top/MVPXmuUIFAQLfQdTpqGi1776942976",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tenjo10ht.top/FXpkGDyUTRqQxEvMSiPD1764033034",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tenjo10vt.top/paKURpJFxJCnukXyqZrN1779133042",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
```

```
        },
        {
            "type": "url",
            "value": "* http://home.tenjp10vs.top/SFyYktVKDQBaqLympWfA1794923063",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.thirtji13ht.top/MwOBqdodAGbyXMofAyrU5986261729",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.thirtjo13sr.top/bYcMGmpHJcbGkomonWsU0126461730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.thirtjo13vt.top/FMmMtBkQtjnpYGvmAcfX3322181730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.thirtjo13vt.top/rvAMJqturkAmDaZoTnSo7412361730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.thirtjo13vt.top/xaDSPDgkqKmDlPNoQLbs1617302014",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventji20ht.top/axNhXgnGYoPSgajZFkaQ5917298626",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventji20vs.top/NWYJPzCYEvZpxoyKvBIK9295321729",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20sr.top/pLDNcrnQYnSceQqdUDvf0117302646",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20vs.top/SOMOJyZWYBxdybbmZeaW1270101730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20vs.top/lwRwtEGztSQcWvXoArFS9063941730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20vt.top/FjnNAcVhtuMKyKxfgwGc3022181730",
            "category": "Network activity",
```

```
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20vt.top/fExmNYmMwsMkeOPpBLzG1620141730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjo20vt.top/ztcbHfsrgDVbKwvjMmcq7417301236",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tventjp20vt.top/julfUeXzXwHcgsxxhkmr6282621730",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelja12sb.top/JLEncoVUzpBxNKNLrTYV1908437312",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelja12sb.top/xKCOYZtRPmSqQvpgghZS1526587311",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12ht.top/OsLGYXbzmZdjCMhTnuGb1972979319",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12ht.top/VqfNYMmqQHyFNagmJCit1767697297",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12ht.top/wUjNbZBIqtyGhfPTmpke1862657298",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12vs.top/YKVZcYkIJkgPraRfOHBr1173008199",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12vs.top/flyGQWUPyIQmXYOpcFMz1866977299",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.twelji12vs.top/nXZUoCnprUWelKqFYScP1053297299",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12ht.top/SHfUuTYBULkoesjZJfWj1573051889",
```

```
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12sr.top/AoVYhzVxzHmClkVkBHzK1964597302",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12sr.top/GDHlEMZKhUWZBxtHkRwh1573028930",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12sr.top/UPMCpUyoKEyLghAHklgZ1473030430",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12vs.top/GGjrrjEDEWQrYYIQCiSz1549107305",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12vs.top/awDRkLatDdHoLFjLkaTk1173065362",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12vt.top/GEZFdXtInPnroqnCxvvX1223677301",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12vt.top/OSVrAwHTMqXZwPLPhTMW1773013581",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljo12vt.top/UrZpabYUoOYCIETTggQp1273022183",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljp12ht.top/HoQpbeizPhmxJmnjugER1397367309",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljp12ht.top/QPoNBSMGOKYXiKKSXopP1257817309",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
            "value": "* http://home.tweljp12ht.top/gwWsuyjcKfHgnGByabIj1771937310",
            "category": "Network activity",
            "comment": "Cryptbot C2 URL"
        },
        {
            "type": "url",
```

```
                "value": "* http://home.tweljp12ht.top/nQVpoVTlTakzyXMzpriM1279757309",
                "category": "Network activity",
                "comment": "Cryptbot C2 URL"
            },
            {
                "type": "url",
                "value": "* http://home.tweljp12vt.top/TLkmyWUrcoKSfuQMaKSm1173082626",
                "category": "Network activity",
                "comment": "Cryptbot C2 URL"
            },
            {
                "type": "url",
                "value": "* http://home.tweljp12vt.top/VszWEchGCZleshrQkPDo1986927307",
                "category": "Network activity",
                "comment": "Cryptbot C2 URL"
            }
        ]
    }
}
```

Source: https://tehtris.com/en/blog/cryptbot-downloader-a-deep-cryptanalysis/