

# PebbleDash - Lazarus / HiddenCobra RAT

[malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html](https://malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html)

malwarenailed

| Type  | Size | Blacklisted ... | Value   |
|-------|------|-----------------|---|
| ascii | 25   | -               | Couldn't create/open file                             |
| ascii | 25   | -               | Failed to allocate memory                             |
| ascii | 21   | -               | Error writing to file                                 |
| ascii | 29   | -               | File not found in the zipfile                         |
| ascii | 24   | -               | Still more data to unzip                              |
| ascii | 35   | -               | Zipfile is corrupt or not a zipfile                   |
| ascii | 18   | -               | Error reading file                                    |
| ascii | 24   | -               | Caller: faulty arguments                              |
| ascii | 52   | -               | Caller: the file had already been partially unzipped  |
| ascii | 47   | -               | Caller: can only get memory of a memory zipfile       |
| ascii | 53   | -               | Caller: not enough space allocated for memory zipfile |
| ascii | 34   | -               | Caller: there was a previous error                    |
| ascii | 52   | -               | Caller: additions to the zip have already been ended  |
| ascii | 42   | -               | Caller: mixing creation and opening of zip            |
| ascii | 46   | -               | Zip-bug: internal initialisation not completed        |
| ascii | 38   | -               | Zip-bug: trying to seek the unseekable                |
| ascii | 46   | -               | Zip-bug: the anticipated size turned out wrong        |
| ascii | 46   | -               | Zip-bug: tried to change mind, but not allowed        |
| ascii | 41   | -               | Zip-bug: an internal error during flation             |
| ascii | 4    | -               | kU'9  |
| ascii | 4    | -               | HMXB  |
| ascii | 4    | -               | ???   |

Hi folks. I was analyzing the PebbleDash malware used by Lazarus APT group. While analyzing the original sample (Md5: d2de01858417fa3b580b3a95857847d5), I was able to find out the C2 server and the port, where it intends to communicate to. I also found an interesting technique it uses to identify the OS version of the victim machine.

During static analysis, I observed interesting strings were starting with "Zip-bug", as can be seen below. Using yara rules I was able to discover some other samples uploaded to HA (Hybrid Analysis) with the same strings embedded. These samples seemed to be not related to d2de01858417fa3b580b3a95857847d5. However, they communicated to South Korea and China.

| Type  | Size | Blacklisted ... | Value   |
|-------|------|-----------------|---|
| ascii | 25   | -               | Couldn't create/open file                             |
| ascii | 25   | -               | Failed to allocate memory                             |
| ascii | 21   | -               | Error writing to file                                 |
| ascii | 29   | -               | File not found in the zipfile                         |
| ascii | 24   | -               | Still more data to unzip                              |
| ascii | 35   | -               | Zipfile is corrupt or not a zipfile                   |
| ascii | 18   | -               | Error reading file                                    |
| ascii | 24   | -               | Caller: faulty arguments                              |
| ascii | 52   | -               | Caller: the file had already been partially unzipped  |
| ascii | 47   | -               | Caller: can only get memory of a memory zipfile       |
| ascii | 53   | -               | Caller: not enough space allocated for memory zipfile |
| ascii | 34   | -               | Caller: there was a previous error                    |
| ascii | 52   | -               | Caller: additions to the zip have already been ended  |
| ascii | 42   | -               | Caller: mixing creation and opening of zip            |
| ascii | 46   | -               | Zip-bug: internal initialisation not completed        |
| ascii | 38   | -               | Zip-bug: trying to seek the unseekable                |
| ascii | 46   | -               | Zip-bug: the anticipated size turned out wrong        |
| ascii | 46   | -               | Zip-bug: tried to change mind, but not allowed        |
| ascii | 41   | -               | Zip-bug: an internal error during flaton              |
| ascii | 4    | -               | kU'9  |
| ascii | 4    | -               | HMXB  |
| ascii | 4    | -               | ??r?  |

While performing dynamic analysis, I observed that the sample uses the API call `IsProcessorFeaturePresent` to determine the version of the victim OS. The `PF_FLOATING_POINT_PRECISION_ERRATA` feature is explicitly set to `FALSE` in x86 version 6.1 and higher.

Assembly snippet showing the `IsProcessorFeaturePresent` call. The instruction `CMP DWORD PTR DS:[4270BC],1` is highlighted, and the comment indicates that the feature `PF_FLOATING_POINT_PRECISION_ERRATA` is set to `FALSE`.

The sample loads several libraries dynamically during run time. This also included `wsock32.dll`. Malware usually does this as an anti-static analysis technique (anti static analysis)

Assembly snippet showing the `connect` function call. The instruction `CALL DWORD PTR DS:[4278C0]` is highlighted, and the comment indicates that the function `ws2_32.connect` is being called. The register `ESI` contains the address `0013FD28`, which is identified as the `sockaddr` structure.

I decoded the "sockaddr" structure which is passed on to the connect function.



terminate processes, and perform target system enumeration.

For a downloadable copy of IOCs, see [MAR-10288834-3.v1.stix](#).

### Submitted Files (1)

aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6 (D2DE01858417FA3B580B3A95857847D5)

### IPs (1)

112.217.108.138

## Findings

aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

### Tags

rootkit trojan

### Details

|      |                                  |
|------|----------------------------------|
| Name | D2DE01858417FA3B580B3A95857847D5 |
| Size | 167937 bytes                     |

PebbleDash inserts fake "server name" in the TLS packet. We can see below some:

The screenshot displays assembly code and memory dump. The assembly code shows a call to 'Kernel32.lstrlen' with a string argument. The memory dump shows a string 'www.avira.com' at address 0013D9E4.

```
0040932D . F7F1 DIV ECX
0040932F . 8955 50FEFF MOV EDI, PTR SS:[EBP-180], EDI
00409335 . 8B95 50FEFF MOV EDI, DWORD PTR SS:[EBP-180]
0040933B . 8B0495 B45C41 MOV EAX, DWORD PTR DS:[EDX*4+425CB4]
00409342 . 50 PUSH EAX
00409349 . FF15 44204200 CALL DWORD PTR DS:[<&KERNEL32.lstrlen>]
0040934F . 66C785 58FE MOV WORD PTR SS:[EBP-1A8], 0
00409358 . 888D 3CFFFF MOV ECX, DWORD PTR SS:[EBP-0C4]
0040935E . 83C1 05 ADD ECX, 5
00409361 . 51 PUSH ECX
00409367 . E8 D9860100 CALL <JMP.&WS2_32.#9>
0040936E . 66:8985 5AFE MOV WORD PTR SS:[EBP-1A6], AX
00409374 . 8B95 3CFFFF MOV EDI, DWORD PTR SS:[EBP-0C4]
00409377 . 83C2 03 ADD EDI, 3
00409379 . 52 PUSH EDI
0040937D . E8 C3860100 CALL <JMP.&WS2_32.#9>
00409384 . 66:8985 5CFE MOV WORD PTR SS:[EBP-1A4], AX
0040938B . C685 5EFEFF MOV BYTE PTR SS:[EBP-1A2], 0
0040938E . 66:8B85 3CFF MOV AX, WORD PTR SS:[EBP-0C4]
00409392 . 50 PUSH EAX
00409399 . E8 A8860100 CALL <JMP.&WS2_32.#9>
[00422044]=75C61977 (KERNEL32.lstrlen)

J 0 FS 0000 0000 0000
T 0 GS 0000 NULL
D 0
O 0 LastErr 00000000 E
EFL 00000246 (NO,NB,E,B
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 43979.0000000
ST7 empty 43979.8536574
3 2 1 0
FST 0020 Cond 0 0 0 0
FCW 027F Prec NEAR,53
Last cmd 0000:0040243A
xmm0 00000000 00000000
xmm1 00000000 00000000
xmm2 00000000 00000000
xmm3 00000000 00000000
xmm4 00000000 00000000
xmm5 00000000 00000000
xmm6 00000000 00000000
xmm7 00000000 00000000
xmm8 00000000 00000000
xmm9 00000000 00000000
xmm10 00000000 00000000
xmm11 00000000 00000000
xmm12 00000000 00000000
xmm13 00000000 00000000
xmm14 00000000 00000000
xmm15 00000000 00000000
xmm16 00000000 00000000
xmm17 00000000 00000000
xmm18 00000000 00000000
xmm19 00000000 00000000
xmm20 00000000 00000000
xmm21 00000000 00000000
xmm22 00000000 00000000
xmm23 00000000 00000000
xmm24 00000000 00000000
xmm25 00000000 00000000
xmm26 00000000 00000000
xmm27 00000000 00000000
xmm28 00000000 00000000
xmm29 00000000 00000000
xmm30 00000000 00000000
xmm31 00000000 00000000
xmm32 00000000 00000000
xmm33 00000000 00000000
xmm34 00000000 00000000
xmm35 00000000 00000000
xmm36 00000000 00000000
xmm37 00000000 00000000
xmm38 00000000 00000000
xmm39 00000000 00000000
xmm40 00000000 00000000
xmm41 00000000 00000000
xmm42 00000000 00000000
xmm43 00000000 00000000
xmm44 00000000 00000000
xmm45 00000000 00000000
xmm46 00000000 00000000
xmm47 00000000 00000000
xmm48 00000000 00000000
xmm49 00000000 00000000
xmm50 00000000 00000000
xmm51 00000000 00000000
xmm52 00000000 00000000
xmm53 00000000 00000000
xmm54 00000000 00000000
xmm55 00000000 00000000
xmm56 00000000 00000000
xmm57 00000000 00000000
xmm58 00000000 00000000
xmm59 00000000 00000000
xmm60 00000000 00000000
xmm61 00000000 00000000
xmm62 00000000 00000000
xmm63 00000000 00000000
xmm64 00000000 00000000
xmm65 00000000 00000000
xmm66 00000000 00000000
xmm67 00000000 00000000
xmm68 00000000 00000000
xmm69 00000000 00000000
xmm70 00000000 00000000
xmm71 00000000 00000000
xmm72 00000000 00000000
xmm73 00000000 00000000
xmm74 00000000 00000000
xmm75 00000000 00000000
xmm76 00000000 00000000
xmm77 00000000 00000000
xmm78 00000000 00000000
xmm79 00000000 00000000
xmm80 00000000 00000000
xmm81 00000000 00000000
xmm82 00000000 00000000
xmm83 00000000 00000000
xmm84 00000000 00000000
xmm85 00000000 00000000
xmm86 00000000 00000000
xmm87 00000000 00000000
xmm88 00000000 00000000
xmm89 00000000 00000000
xmm90 00000000 00000000
xmm91 00000000 00000000
xmm92 00000000 00000000
xmm93 00000000 00000000
xmm94 00000000 00000000
xmm95 00000000 00000000
xmm96 00000000 00000000
xmm97 00000000 00000000
xmm98 00000000 00000000
xmm99 00000000 00000000
xmm100 00000000 00000000
xmm101 00000000 00000000
xmm102 00000000 00000000
xmm103 00000000 00000000
xmm104 00000000 00000000
xmm105 00000000 00000000
xmm106 00000000 00000000
xmm107 00000000 00000000
xmm108 00000000 00000000
xmm109 00000000 00000000
xmm110 00000000 00000000
xmm111 00000000 00000000
xmm112 00000000 00000000
xmm113 00000000 00000000
xmm114 00000000 00000000
xmm115 00000000 00000000
xmm116 00000000 00000000
xmm117 00000000 00000000
xmm118 00000000 00000000
xmm119 00000000 00000000
xmm120 00000000 00000000
xmm121 00000000 00000000
xmm122 00000000 00000000
xmm123 00000000 00000000
xmm124 00000000 00000000
xmm125 00000000 00000000
xmm126 00000000 00000000
xmm127 00000000 00000000
xmm128 00000000 00000000
xmm129 00000000 00000000
xmm130 00000000 00000000
xmm131 00000000 00000000
xmm132 00000000 00000000
xmm133 00000000 00000000
xmm134 00000000 00000000
xmm135 00000000 00000000
xmm136 00000000 00000000
xmm137 00000000 00000000
xmm138 00000000 00000000
xmm139 00000000 00000000
xmm140 00000000 00000000
xmm141 00000000 00000000
xmm142 00000000 00000000
xmm143 00000000 00000000
xmm144 00000000 00000000
xmm145 00000000 00000000
xmm146 00000000 00000000
xmm147 00000000 00000000
xmm148 00000000 00000000
xmm149 00000000 00000000
xmm150 00000000 00000000
xmm151 00000000 00000000
xmm152 00000000 00000000
xmm153 00000000 00000000
xmm154 00000000 00000000
xmm155 00000000 00000000
xmm156 00000000 00000000
xmm157 00000000 00000000
xmm158 00000000 00000000
xmm159 00000000 00000000
xmm160 00000000 00000000
xmm161 00000000 00000000
xmm162 00000000 00000000
xmm163 00000000 00000000
xmm164 00000000 00000000
xmm165 00000000 00000000
xmm166 00000000 00000000
xmm167 00000000 00000000
xmm168 00000000 00000000
xmm169 00000000 00000000
xmm170 00000000 00000000
xmm171 00000000 00000000
xmm172 00000000 00000000
xmm173 00000000 00000000
xmm174 00000000 00000000
xmm175 00000000 00000000
xmm176 00000000 00000000
xmm177 00000000 00000000
xmm178 00000000 00000000
xmm179 00000000 00000000
xmm180 00000000 00000000
xmm181 00000000 00000000
xmm182 00000000 00000000
xmm183 00000000 00000000
xmm184 00000000 00000000
xmm185 00000000 00000000
xmm186 00000000 00000000
xmm187 00000000 00000000
xmm188 00000000 00000000
xmm189 00000000 00000000
xmm190 00000000 00000000
xmm191 00000000 00000000
xmm192 00000000 00000000
xmm193 00000000 00000000
xmm194 00000000 00000000
xmm195 00000000 00000000
xmm196 00000000 00000000
xmm197 00000000 00000000
xmm198 00000000 00000000
xmm199 00000000 00000000
xmm200 00000000 00000000
xmm201 00000000 00000000
xmm202 00000000 00000000
xmm203 00000000 00000000
xmm204 00000000 00000000
xmm205 00000000 00000000
xmm206 00000000 00000000
xmm207 00000000 00000000
xmm208 00000000 00000000
xmm209 00000000 00000000
xmm210 00000000 00000000
xmm211 00000000 00000000
xmm212 00000000 00000000
xmm213 00000000 00000000
xmm214 00000000 00000000
xmm215 00000000 00000000
xmm216 00000000 00000000
xmm217 00000000 00000000
xmm218 00000000 00000000
xmm219 00000000 00000000
xmm220 00000000 00000000
xmm221 00000000 00000000
xmm222 00000000 00000000
xmm223 00000000 00000000
xmm224 00000000 00000000
xmm225 00000000 00000000
xmm226 00000000 00000000
xmm227 00000000 00000000
xmm228 00000000 00000000
xmm229 00000000 00000000
xmm230 00000000 00000000
xmm231 00000000 00000000
xmm232 00000000 00000000
xmm233 00000000 00000000
xmm234 00000000 00000000
xmm235 00000000 00000000
xmm236 00000000 00000000
xmm237 00000000 00000000
xmm238 00000000 00000000
xmm239 00000000 00000000
xmm240 00000000 00000000
xmm241 00000000 00000000
xmm242 00000000 00000000
xmm243 00000000 00000000
xmm244 00000000 00000000
xmm245 00000000 00000000
xmm246 00000000 00000000
xmm247 00000000 00000000
xmm248 00000000 00000000
xmm249 00000000 00000000
xmm250 00000000 00000000
xmm251 00000000 00000000
xmm252 00000000 00000000
xmm253 00000000 00000000
xmm254 00000000 00000000
xmm255 00000000 00000000
xmm256 00000000 00000000
xmm257 00000000 00000000
xmm258 00000000 00000000
xmm259 00000000 00000000
xmm260 00000000 00000000
xmm261 00000000 00000000
xmm262 00000000 00000000
xmm263 00000000 00000000
xmm264 00000000 00000000
xmm265 00000000 00000000
xmm266 00000000 00000000
xmm267 00000000 00000000
xmm268 00000000 00000000
xmm269 00000000 00000000
xmm270 00000000 00000000
xmm271 00000000 00000000
xmm272 00000000 00000000
xmm273 00000000 00000000
xmm274 00000000 00000000
xmm275 00000000 00000000
xmm276 00000000 00000000
xmm277 00000000 00000000
xmm278 00000000 00000000
xmm279 00000000 00000000
xmm280 00000000 00000000
xmm281 00000000 00000000
xmm282 00000000 00000000
xmm283 00000000 00000000
xmm284 00000000 00000000
xmm285 00000000 00000000
xmm286 00000000 00000000
xmm287 00000000 00000000
xmm288 00000000 00000000
xmm289 00000000 00000000
xmm290 00000000 00000000
xmm291 00000000 00000000
xmm292 00000000 00000000
xmm293 00000000 00000000
xmm294 00000000 00000000
xmm295 00000000 00000000
xmm296 00000000 00000000
xmm297 00000000 00000000
xmm298 00000000 00000000
xmm299 00000000 00000000
xmm300 00000000 00000000
xmm301 00000000 00000000
xmm302 00000000 00000000
xmm303 00000000 00000000
xmm304 00000000 00000000
xmm305 00000000 00000000
xmm306 00000000 00000000
xmm307 00000000 00000000
xmm308 00000000 00000000
xmm309 00000000 00000000
xmm310 00000000 00000000
xmm311 00000000 00000000
xmm312 00000000 00000000
xmm313 00000000 00000000
xmm314 00000000 00000000
xmm315 00000000 00000000
xmm316 00000000 00000000
xmm317 00000000 00000000
xmm318 00000000 00000000
xmm319 00000000 00000000
xmm320 00000000 00000000
xmm321 00000000 00000000
xmm322 00000000 00000000
xmm323 00000000 00000000
xmm324 00000000 00000000
xmm325 00000000 00000000
xmm326 00000000 00000000
xmm327 00000000 00000000
xmm328 00000000 00000000
xmm329 00000000 00000000
xmm330 00000000 00000000
xmm331 00000000 00000000
xmm332 00000000 00000000
xmm333 00000000 00000000
xmm334 00000000 00000000
xmm335 00000000 00000000
xmm336 00000000 00000000
xmm337 00000000 00000000
xmm338 00000000 00000000
xmm339 00000000 00000000
xmm340 00000000 00000000
xmm341 00000000 00000000
xmm342 00000000 00000000
xmm343 00000000 00000000
xmm344 00000000 00000000
xmm345 00000000 00000000
xmm346 00000000 00000000
xmm347 00000000 00000000
xmm348 00000000 00000000
xmm349 00000000 00000000
xmm350 00000000 00000000
xmm351 00000000 00000000
xmm352 00000000 00000000
xmm353 00000000 00000000
xmm354 00000000 00000000
xmm355 00000000 00000000
xmm356 00000000 00000000
xmm357 00000000 00000000
xmm358 00000000 00000000
xmm359 00000000 00000000
xmm360 00000000 00000000
xmm361 00000000 00000000
xmm362 00000000 00000000
xmm363 00000000 00000000
xmm364 00000000 00000000
xmm365 00000000 00000000
xmm366 00000000 00000000
xmm367 00000000 00000000
xmm368 00000000 00000000
xmm369 00000000 00000000
xmm370 00000000 00000000
xmm371 00000000 00000000
xmm372 00000000 00000000
xmm373 00000000 00000000
xmm374 00000000 00000000
xmm375 00000000 00000000
xmm376 00000000 00000000
xmm377 00000000 00000000
xmm378 00000000 00000000
xmm379 00000000 00000000
xmm380 00000000 00000000
xmm381 00000000 00000000
xmm382 00000000 00000000
xmm383 00000000 00000000
xmm384 00000000 00000000
xmm385 00000000 00000000
xmm386 00000000 00000000
xmm387 00000000 00000000
xmm388 00000000 00000000
xmm389 00000000 00000000
xmm390 00000000 00000000
xmm391 00000000 00000000
xmm392 00000000 00000000
xmm393 00000000 00000000
xmm394 00000000 00000000
xmm395 00000000 00000000
xmm396 00000000 00000000
xmm397 00000000 00000000
xmm398 00000000 00000000
xmm399 00000000 00000000
xmm400 00000000 00000000
xmm401 00000000 00000000
xmm402 00000000 00000000
xmm403 00000000 00000000
xmm404 00000000 00000000
xmm405 00000000 00000000
xmm406 00000000 00000000
xmm407 00000000 00000000
xmm408 00000000 00000000
xmm409 00000000 00000000
xmm410 00000000 00000000
xmm411 00000000 00000000
xmm412 00000000 00000000
xmm413 00000000 00000000
xmm414 00000000 00000000
xmm415 00000000 00000000
xmm416 00000000 00000000
xmm417 00000000 00000000
xmm418 00000000 00000000
xmm419 00000000 00000000
xmm420 00000000 00000000
xmm421 00000000 00000000
xmm422 00000000 00000000
xmm423 00000000 00000000
xmm424 00000000 00000000
xmm425 00000000 00000000
xmm426 00000000 00000000
xmm427 00000000 00000000
xmm428 00000000 00000000
xmm429 00000000 00000000
xmm430 00000000 00000000
xmm431 00000000 00000000
xmm432 00000000 00000000
xmm433 00000000 00000000
xmm434 00000000 00000000
xmm435 00000000 00000000
xmm436 00000000 00000000
xmm437 00000000 00000000
xmm438 00000000 00000000
xmm439 00000000 00000000
xmm440 00000000 00000000
xmm441 00000000 00000000
xmm442 00000000 00000000
xmm443 00000000 00000000
xmm444 00000000 00000000
xmm445 00000000 00000000
xmm446 00000000 00000000
xmm447 00000000 00000000
xmm448 00000000 00000000
xmm449 00000000 00000000
xmm450 00000000 00000000
xmm451 00000000 00000000
xmm452 00000000 00000000
xmm453 00000000 00000000
xmm454 00000000 00000000
xmm455 00000000 00000000
xmm456 00000000 00000000
xmm457 00000000 00000000
xmm458 00000000 00000000
xmm459 00000000 00000000
xmm460 00000000 00000000
xmm461 00000000 00000000
xmm462 00000000 00000000
xmm463 00000000 00000000
xmm464 00000000 00000000
xmm465 00000000 00000000
xmm466 00000000 0000000
```