HZ RAT goes China. Walking down the Royal Road as we did… | by DCSO CyTec Blog | Nov, 2022

medium.com/@DCSO_CyTec/hz-rat-goes-china-506854c5f2e2

DCSO CyTec Blog November 16, 2022

DCSO CyTec Blog

Nov 16

.

15 min read

HZ RAT goes China

Walking down the Royal Road as we did in one of our previous posts, another by-catch of our Yara rule caught our attention. Turns out we found HZ Rat — a lesser known Trojan.

Source: ❤
The malware we analyse in this article initially aroused curiosity because the payload of the RTF document did not match the pattern we had previously observed in relation to the deployed Yara hunt. Furthermore, the dropped binary shows interesting behaviour as it does not contact the C2 server via domain requests and instead exclusively uses a mix of public and private IP addresses. Especially the use of private IP addresses to contact the C2 server seems uncommon.

First OSINT research of the malware lead to no results regarding public reports or analysis reports. Only Rising, a Chinese security company, seems to know more, given that they published an AV signature for it. Therefore, the malware we analyse in the this article can be identified as "Backdoor.HZRat!1.DB91 (CLASSIC)", defining the name of the malware as "HZ Rat".

In this article we analyse HZ Rat and try to connect the breadcrumbs we found along this way. We discuss the distribution methods, visualise the timeline of the campaign and communicate with C2 servers.

Blog authored by and

Distribution

The threat actor utilises two different attack chains to deliver the backdoor to its victims. Either embedded as self-extracting zip archive or as malicious RTF document build presumably with the Royal Road framework.

Two ways to deliver HZ Rat.

RTF documents

The first distribution method used is an RTF document. The document itself contains no content, images or text and only the lure filename is used to social engineer the victims into opening the document. Once opened, the document writes HZ Rat to disk as *default.exe* and executes it with an Equation Editor exploit (CVE-2017–11882) hidden in the document and triggered after opening the document.

The process tree below illustrates how the document executes the payload. A more in-depth explanation of the Equation Editor exploit (CVE-2017–11882) and how it works can be found in one of our previous posts here.

Process tree for
Based on the Equation Editor exploit-object we identified a long list of documents on VirusTotal which are all linked to HZ Rat samples indicating a regular use as shown below:

This of the EquationEditor exploit reveals other malicious documents delivering HZ Rat.s

7zS.sfx — Self Extracting Zip Archive

The second distribution method simply piggybacks on the archive extraction process after tricking a user into executing a malicious self extracting archive. Pretending that the archive installs OpenVPN, puTTYgen or EasyConnect, the archive actually executes *install.vbs* which first runs the contained *default.exe* (HZ Rat) and afterwards the actual lure program. The content of *install.vbs* is kept simple as shown below:

```
Set objArgs = Wscript.ArgumentsDim shlSet shl = CreateObject("Wscript.Shell")Call
shl.Run("cmd /K " & objArgs(0) & " & exit", 0, false)Call shl.Run(objArgs(1))Set shl
= NothingWscript.Quit
```

The process tree below illustrates this behaviour as well. The initial filename “VPN登录控件.exe” roughly translates to “VPN Login Control.exe”.

Process tree for

Same Sample In Both Attack Chains

During our analysis, we noticed that some samples are used in both attack chains which allowed us to connect both attacks to one campaign.

HZ Rat Analysis

Given that we couldn’t find any research on HZ Rat online, the following section briefly analyses the malware and lists its capabilities.

The PDB Path

Our list of collected samples can be divided into plain and packed samples of which at the time of writing the group of plain samples is slightly larger but a trend towards packed samples is clearly identifiable. The plain samples come in handy with the PDB path included and, what we believe, the version number. In some instances, the PDB path also contains presumably the project name “hp_client_win” as shown in the block below:

```
D:\WORKSPACE\\hp_client_win\Trojan\x64\Release\Trojan.pdbD:\WORKSPACE\\Trojan\x64\Rele
```

The PDB path appears to be the reason why Rising named their AV signatures HZ Rat. For most of the samples we identified, the following Rising AV signatures triggered as well:

- “Backdoor.HZRat!1.DB91 (C64:YzY0OiTdg76jwZSL)”,
- “Backdoor.HZRat!1.DB91 (C64:YzY0Ol8Gio2fTy+DE6K09G2bPqs)”,
- “Backdoor.HZRat!1.DB91 (CLASSIC)”,
- “Backdoor.HZRat!1.DB91 (CLOUD)”,

Based on the collected samples, there are at least three versions of HZ Rat available, which are `HZ_2.8.2`, `HZ_2.9.0`, `HZ_2.9.1` as well as the packed HZ Rat versions which don’t contain the PDB path anymore.

Capabilities and Protocol

The malware itself is kept very simple. Once started, it iterates through a list of C2 servers in order to connect and receive commands. The malware itself behaves like a client and simple executes received commands. Once connected, the C2 server sends one of five possible commands listed below:

```
* execute PowerShell command and send STDOUT to C2* execute PowerShell script and
send content of specified temp file to C2* write file to disk* upload file to C2*
ping (appears to be buggy)
```

The communication protocol itself is custom. It requires a specific “handshake” pattern (referred as “Cookie” in the malware) in order to initiate the communication with the C2 server. Beside this, the communication itself is XOR encrypted using the key 0x42.

Custom communication pattern sent from the client to initiate the C2 server communication

Custom Packers

In the early days of July 2022, we detected the first versions of packed HZ Rat samples. The packer itself is custom and initially only encoded the payload with Base64, which we referenced as *packed_base64_v1*. The packer evolved shortly after detection to a slightly more enhanced Base64 packer, which we identify as *packed_base64_v2*. The last known version uses AES to encrypt its payload. We reference this packer as *packed_aes_v1*.

During our analysis, we generally extracted samples packed with the first version (*packed_base64_v1*) with a simple bash script approach as shown in the screenshot below.

Simple Base64 unpacking command for

The bash script approach did not work for samples packed with *packed_base64_v2* and *packed_aes_v1* which is why we wrote custom unpacking tools for both packer variants. We share the unpacker here.

The packer architecture to unpack the AES encrypted data and to execute the payload is quite simple as shown in the screenshot below. The library used for AES decryption is WjCryptLib.

Architecture of the AES packer executing the payload
Below we share an example list of samples of the packed HZ Rat variants:

```
# packed_base64_v1 (Bash command unpacking):
8ba90d91eea87f6f7b9df4010b038dd2692b62777677f421f7d1003f28f29bb4



# packed_base64_v2 (Base64 unpacker):
b4670afde3e88951274780f2128c9584ef80813293ac64c69225fac3926e71ee

# packed_aes_v1 (AES
unpacker):e350dc55f61eda0a7372fb5bbf35fac6d8c928912f3bef75efeaca7c1338093f
```

Campaign

Alongside the malware analysis, we started searching for more HZ Rat samples. For this, we created and deployed Yara rules on VirusTotal which we share here. Based on this rule, we were able to identify more than 120 HZ Rat samples spread over the last two years.

In an attempt to visualise the discovered data set, we created a time graph based on the *creation_date* timestamp of each sample and the correlating *first_submission_date* of the sample to VirusTotal. While the *creation_date* timestamp could be tempered with, it does not appear to be in this case. The resulting graph below provides a rough view into the operational time of the malware. The graph indicates a constant use and development process of the malware of time.

How to read the graph: Each horizontal line in the graph connects an HZ Rat sample's creation timestamp (shade of red/black) to its first submission timestamp (green)

The diagram above illustrates the HZ Rat versions `HZ_2.8.2`, `HZ_2.9.0` and `HZ_2.9.1` in shades of red/black over time. The graph indicates that the HZ Rat samples are built on fixed dates. We believe that the malware was created only once in a while or once per version. This "gold sample" then gets copied as needed and only the C2 IP addresses are patched into it afterwards. The second graph below adds the creation timestamp of the corresponding distribution method files, which seem to be created earlier but used in the same copy, paste, patch approach as HZ Rat. The gaps between creation date and first submission date of each sample frames the period of malware deployment.

“Creation times” of the related delivery method added to HZ Rat overview
The shortest creation date to VirusTotal first submission ratio is listed below:

```
HZ packed - bb540a1e357b50e406e07f35993471dec1b8502961301e7984581134518c40a4HZ packed
- 5b40c2e609ec90fcfd4e0be7b642f8b7bc6bd552801caea2b9d1fdd6992b6982HZ packed -
eac8587a6b5a1ed5b652bf8440afff90da3b846cec63a5d4f755a1a5fa87b375HZ packed -
dd153c8c59bf3e47b894da9777c25424bb9b7e16686010378098d207646c6a42HZ packed -
6abe974c807a03f81ad3e7ba7ff7695b30c450733533ff9df733c3050e74a368HZ packed -
a4574b3df09d3c62d780693e71031a8d5d656ed933dbc07be8175249cb7ccacaHZ packed -
85b6664c386c2c9cd7d0a8a6dc08c281c814669bdb75f02e5b24d1f893eaae69HZ packed -
431fc223b302150ef2ab549c9ae8f96cb964a73aa1a860279d2b0f9039f09e2eHZ packed -
05d2668a9b80f58bc5b05f3e705aac60f05268ec8ed68b302104e2b5ee4fdf3fHZ packed -
5b37a1144e92a20c2d7c44d1ee896be8635d56d7b03a74f0e89e13e69f63e343
```

Command and Control Servers

Having the malware analysed and the campaign visualised, we switched our focus to the C2 servers. For this, we wrote a C2 server extractor to extract all C2 server addresses from the samples we previously collected and to compile a large list of all known C2 servers and related ports. We share the extractor here. Remarkable on this list is the mix of private and public IP addresses. We also noticed that all possible combinations of private and public IPs are available in single HZ Rat samples. Listed below are samples with C2 server lists to represent all possible private/public IP combinations:

```
C2 servers - public IPs only:
- Sample:
  * 41bf15434e1b417692edfc46395b0ca867b7af0a99f42256760c9de92d1a7d1d
- IP:
  * 10.8.8.190:8081



C2 servers - private IPs only:
- Sample:
  * 8288d98084d63d1c0955d2393540c8638adadca7befedd5315e0cb3bd92be3fa
- IP:
  * 192.168.110.140:8081

C2 servers - private and public IPs:- Sample:   *
f27cd021ba45e3b1070a380fa6be2204cebbdf98ae6d38d90560b1f1bb6c0195- IP:  *
114.113.238.83:9000  * 221.195.106.200:9090  * 192.168.210.179:8081  *
192.168.211.20:8081  * 192.168.211.10:8081  * 192.168.218.128:8090
```

Server Availability Check

For a better understanding we generated a heat map of all known C2 sever locations. The map clearly visualises a focus on China. Less than five C2 servers per country where also located in Russia, Australia, United States, Netherlands and Spain.

C2 server distribution globally.
Our next analysis step after compiling the list of IP addresses was to contact all C2 servers and to find out whether any of them are still online. To do so, we re-implemented parts of the communication protocol and the initial handshake required to establish the connection. The scan revealed that more than 10 servers are still online and even respond. This indicates that the campaign is long running and still active. The screenshot below provides the output of our C2 server scan including the start of the server responses.

Scanning for HZ Rat servers and evaluating first response packet— scanned 2022–08–02
For the sake of completeness, the list of responding C2 servers is shown below:

```
Online 106[.]120.215.202:8089Online 114[.]113.238.83:9000Online
114[.]113.238.84:6523Online 114[.]251.223.84:8081 # oa.pumch.cnOnline
116[.]54.125.202:8081Online 116[.]6.102.21:8081Online 124[.]250.18.111:8080Online
218[.]22.14.11:8081Online 220[.]248.250.19:8081 # sgwpdm.ah.sgcc.com.cnOnline
222[.]85.157.82:8081Online 58[.]240.32.125:8081Online 61[.]144.203.171:8081
```

Server Response

Shortly after identifying the C2 servers and checking their availability, we noticed that it is possible to extract the full command list from the C2 servers by implementing the whole communication protocol in order to keep the communication ongoing. The command list then allows us to learn more about the actual attack. We share our proof-of-concept C2 scanner here.

The list below provides a communication stream we received with our protocol re-implementation. We always responded with a packet containing “HMRAM5ZSOL”, which is the reason why some paths and requests from the server also contain “HMRAM5ZSOL” and appear to be out of context.

Received and decrypted C2 server communication
Reviewing the received commands indicates that, beside system reconnaissance, a strong focus is set on credential dumping. Noteworthy are the regional target indicators like attempts to copy files from folders such as `Tencent Files` or `Wechat Files`. In general, the attacker aims to acquire data from various locations and applications. This includes credentials for:

- `PremiumSoft` which we assume aims for ,
- filenames containing `wxid` which we assume is related to ,
- `.aggressor.prop` which contains credentials,
- `.gitconfig` which contains credentials,

- stored credentials in,
- stored credentials in
- stored credentials in
- `logins.json` and `key4.db` indicating

At an early stage of our analysis we decrypted the full communication flow of an HZ Rat sandbox run which we found as PCAP file provided by Zenbox on VirusTotal. We share an example of the decrypted communication here and our PoC PCAP decryptor here.

Miscellaneous

Along our analysis path, we discovered puzzle pieces of HZ Rat we cannot link to the analysis path above. We still want to mention them in the following section to keep it documented to help other analysts later.

China State Construction Engineering Corporation Ltd

One of the samples we found was hosted on `http://oa.cscec[.]com/Customer/posetup.exe` as shown on VirusTotal. CSCEC is known as “China State Construction Engineering Corporation Ltd.”

HZ Rat sample hosted at CSCEC
Beside this, we were able to identify the following domains resolving to HZ Rat C2 server IPs.

```
# We were able to download HZ Rat from the following domains
114[.]251.223.84:8081/default.exe # oa.pumch.cn
116[.]236.40.57:8081/default.exe # finance.yto.net.cn
220[.]248.250.19:8081/default.exe # sgwpdm.ah.sgcc.com.cn

# Domain resolved to IP116[.]236.40.57:8081 # finance.yto.net.cn183[.]196.0.25:8081 #
www.hbzyjxkh.cn, hbszyy.gcptrial.com, zhyy.hbszyy.cn218[.]76.15.13:8081 #
dsm.hn.sgcc.com.cn220[.]248.250.19:8081 # sgwpdm.ah.sgcc.com.cn
```

Mutex Gives Cobalt Strike Beacon Away

In addition to the unique PDB path, all versions of HZ Rat use the same mutex `{91E99696-92CC-43F4-99B0-774D80BDAA6B}` to prevent multiple executions on the same system. This mutex gives away a huge list of HZ Rat samples on VirusTotal and allows us to keep track of the campaign. Besides the HZ Rat samples we were able to identify one Cobalt Strike stager with the same mutex and packed with *packed_base64_v1*.

```
Base64 packed Cobalt Strike: Base64 packed Cobalt Strike pdb path:Included Cobalt
Strike sample:extracted Cobalt Strike sample - C2 server:extracted Cobalt Strike
sample - pdb path:
```

Based on the given PDB path, we noticed another group of Cobalt Strike stagers with similar PDB paths contacting the same C2 server as the Cobalt Strike stagers before.

```
* Hash SHA256:* * * * Cobalt Strike sample - C2 server:
```

Another Cobalt Strike stager, this time packed with *packed_base64_v2*.

```
Base64 packed Cobalt Strike (packed_base64_v2):Base64 packed Cobalt Strike pdb
path:extracted Cobalt Strike sample:Cobalt Strike sample - C2 server:Cobalt Strike
sample - pdb path:stripped
```

Conclusion

This article uncovers a campaign previously unknown and undocumented. We identified HZ Rat as payload of malicious RTF documents, found two distribution methods and multiple custom packers. Along our analysis we were able to identify over 120 samples and 3 versions of HZ Rat. We believe that the campaign is still ongoing and active since at least October 2020. HZ Rat itself is used as initial access tool with limited capabilities like command execution and file upload. Our research revealed that this malware was utilised for credential stealing and system reconnaissance.

IoC

Below we share our IoC list. Our tools, the related MISP event and our Yara rules are available on Github as well.

```
# HZ packed
8ba90d91eea87f6f7b9df4010b038dd2692b62777677f421f7d1003f28f29bb4
15a3175f0097386f617c33fb2552dc8e5972055bb4ff99ef8532763e248543b7
b4670afde3e88951274780f2128c9584ef80813293ac64c69225fac3926e71ee
eac8587a6b5a1ed5b652bf8440afff90da3b846cec63a5d4f755a1a5fa87b375
7ba72fa840bcf6de6fb780cfd6593f14507d8e8790eeb8cbac56cafe14a7e5f5
cda5c0fad26119c50ef063dfb3c6bd666877e564d31b64341486298cc9568242
eb95965f10efca15fc021f879923679a7acb2302ed1211d4d08529efc10a73a9
2ca22a75575f63575f87f653780367058f90bce24a77876c16d927f747f78afd
5da049fb045f8eb7865db8d51b54769035974444534bbc23c965e55f29f70b58
2cedea36bbdc44d8ec83acf86c18f867547c8c53ebb234a4b2c8eed4e9ecac16
7cbb19d3ea54309167b4d09cfb0562313aa3b0822637b7449e05f8ab603d30e4
94fd1888e349ca100fcc557e446538e1524f3d6e36b234f39d9075414118e95f
d5763310b90a82cf8754892c61442746db57cb169c639dd2bc0ceb989c6222a5
a16734ffb1895423dd39ee243dcd7a867936568d4ec006fadc8f55d74aa742cd
74f0271fbfb86fbcb0370b3b9de8845cc8a8f7a1be1536d131da724bc5128db4
7bfe5a1a31db7a1de7f42dc35b02797c4d29ae079c525404470f85b5a4a46283
97114be15a56f10225e1605284e568adeb2c5bef4f6941cb8da3cd20c389305f
195459fdb0ca5b775e864a69f47a0acd5761f56777e29d3e09a84420362248b7
327ffcc9ddb5748cdf3b2c43c7a2fc2778e86ee69649c7c692253699f713ee91
ebce7218348ad7292c7c3bbbcf7246ad24827a3c040622895b8ce3880d8e0516
410004b8ef0096e4029def96895ef4cea89e1e41e3113ef995ab9c19de39782b
ca0ecb347f6d877e40272f43d203c12603087b8102757686c0162bcc770b4ec9
b75a1ef557e02d243b77dbf5c5361d3a702b6b13108f4df631f565b8191fe652
05d2668a9b80f58bc5b05f3e705aac60f05268ec8ed68b302104e2b5ee4fdf3f
e8ef31de4a5e751ec1c8fc8a41b48030e3f3e9cf466eafd250574127e5b1107c
5f5388bf011eb01702b3ea01a994b1d0a666448d61a4bd70bbc048f2dfb3b386
64f46b97eb19b750b9fbd97a786ef5ea050ffe65ea6b09eef2be23d7b10a6987
cffcae49f944635ab86518e172a516f15c6ad8300b168243371c20893bdf90ba
e81d27b7132a18d58693b41b18f24e70e63c5b8366acde4c05f8a4d7800e0fcc
e36a5ed08916d63efc5bc1d2ccf7e7185fc13b72d744339cc89552d6f8ebc9cd
1d8be308521bda4857742a2fb9ef65020126e5f623ef2540c3a3ab999c4578b6
a880a9ebfcdeed5a8180969bc34a2d9861580ecfff6d63f8a4d223541284f17b
d4940f74664a1571964fba1a4e0a7a070f5cbfeb2e1f2823c3e51b8677a002f4
02878538eda1b69cc276332943b580fde422bf413728cbfb872b72fd06170a7b
ff4bb86a4d728c1334987084e2aca4e06973da20b5dc4fcba1394376910fb584
bb540a1e357b50e406e07f35993471dec1b8502961301e7984581134518c40a4
43633be77bf48025fa74409e45dc2f9ebacce5d8e915d98b965b919592c4e357
b246c5e739d19041d5643a58f1d421d93578203ace87b24bc92eda8fe7f43a57
c1488c2a93975f89eefe0652e2955d629a20a20d8f24a8f0330d21eaa1122942
daa9d237c0d35b658fd190b01f04a9fe0e0ff630d53044171b71841da6e73b93
f0e00c806cda1d8fb5618c2bdc5275392f8065cb271fda2cb29bc74fda0f589b
ce7dbc382bbe039a461cd946ed51ef96940f709faeed2c6b6a270d31e06ca187
8a783d6397a6acff33cbae51cae7b9a1d7dbb1ec4c36fe78f2d6cdc76ece372e
df6470efe8ef0a75c95a1e46f89149baaf5369676bf05390f5e7bb140f6eaba0
448469af181da35ea187613754fa0ce5f5ba2a3b57062d0ed0d1e2695c46c52d
5b40c2e609ec90fcfd4e0be7b642f8b7bc6bd552801caea2b9d1fdd6992b6982
dd153c8c59bf3e47b894da9777c25424bb9b7e16686010378098d207646c6a42
85b6664c386c2c9cd7d0a8a6dc08c281c814669bdb75f02e5b24d1f893eaae69
431fc223b302150ef2ab549c9ae8f96cb964a73aa1a860279d2b0f9039f09e2e
a4574b3df09d3c62d780693e71031a8d5d656ed933dbc07be8175249cb7ccaca
d532c5f614b296600b5e59d8c740d370587809abf3457871ab25e02d310b05a7
```

```
82bf73b30c2c8cdf1d99325820b93f2564e82960154e19d6108b168de0d0999a
e350dc55f61eda0a7372fb5bbf35fac6d8c928912f3bef75efeaca7c1338093f
9e22fe08d2543952b8939f3f830870e46ceae0443bfb316bca4896d12a20b6b1
ba10cd8c7534e6b6f15976c68f85532bc4a95522b1ff9255372195aa4ecafd28
07c27522de40dcf482c9259090f56cb17f512295a0c63de8e7394b3aa593b0f0
6abe974c807a03f81ad3e7ba7ff7695b30c450733533ff9df733c3050e74a368
dd833d5a522abd6748ead5ae9c5ca329b5c26822fcc9dd00a4103a43705ef328
2a530e56076897ed6de33554b350bff9825e663b28d67a6417ba17740860a2db
7dac6ed39734927d545eea3f06a368dd3bfaea1da5a633de0c7ea25f30aeabdf
5b37a1144e92a20c2d7c44d1ee896be8635d56d7b03a74f0e89e13e69f63e343
66336920db1c60ce7286790473defa5b9ffd9a91116a5d0a91e4a968f5270f76
```

```
# HZ_2.8.2
afac99afaf3298b8663e52effad48a8229f8b89c5b36700e70f1b008c73a0ee5
df172da36e208dd34c6e31f9c6d1ec6ebfef32a5d97bfa181320a9d016d6774a
0fd954e54d9cff03a150eb2828cde9eb5b757562729bcb37a14722e726ae5f72
48cd5e774c0bcb6ad8cac3a8b8aa4c984f2bae9ecc42a380fb3643c120887a3d
163038221270cf4f0064c2306a1ff8ec82dc17201fd595d10126a564c97e9028
22fc6213f13e03dea792a3a47b633db52de542af2cdca54023dbe816ea49191e
43dc6e53483d76b6c212e5deb527cf67bf88ce8a9e0b0e0f25511a2c74a9242a
d2d1f0e2848ad5935be0a22a484f96c6bd5ec6c0900f1fc304e315e98ebedea1
40cd43e05916077d5f7d6b95f103eb9c9d93b132a10dd9f06c7c933742525be5
6ae4342e2f3dfe7ffc4febb57faa60c4fede8412708af4e42c72f28788be98f5
cf0287add7f389a8e02c1dec44101cdb3db67fd139c71f64c2cee4114d828990
ccd8d51b0658282a2a676b80bd0a210bf9462d15f5e5414099ecde5c6a22028b
0568a2a26842ea0820f466c54a354400a3331569ee0d58186affaa2b937788c0
cd576dc0140033a55423992f1a08f06e8db94e6bcc8646dbeb81b9094c51c541
9a1b02896e7d7175cfb76573d30ae178b3943d6f45043ee3e572b6db3c8fa00d
30854cac5deb9c3baf91597e65f804369d0ad2f962ffa462464bf9770a99241e
cb3e71a91e832a6b4c82a3c4a993f89d2285e0236aea0dcb99c475eaa7821458
dc06077246fdbe9d0589bd1bbf4b691eb14d1dc036fa845c4d9ceae8301c117c
d641fc39cedcbe816b6a4b602990a87ce6184a27f62d0d37839c9a7ae02e6630
f6311d5c398e7d530e045e24ea67a031a7d9f30e05a8e7646eb239b9aab36527
0211df6bbf16b28941a3af808bfcf2fd3ad00cac120ce778acc09a4997b7734b
12c0024b55da926aa0b87158151687ddf94e9f1f65d80c9e121d718cb2559c96
1f7b11abf5ca8e96939a5a8ac3d1dcfff352ea10c6f48b3685c25157146ff414
5eac7c9ade0ecc246d7b240970f877f760e1bd0f651b954afd3b3a8d7c29597f
1603e2a2876c467cd4001bc8dc333f8f3ceeac4adbf6a1d14919bb5a363a043f
d16b637a27aada1e281d59c664f08db031128fecd95ca199bc7b11e5541d9ebd
0afaeaa3eee2f90e6fbda2322a65376dd977bd529c0127d6b309a56122ba63bb
4e5d0b9f0608e3cb29e89e3765961299df7cfcd03a1ea2dcd15c36bc28bebb0c
4e580427fed51a485cbeb1f28af5109890835080340df0ca9c41aab4dc6f3910
826deb513651c2cb043414f05ab54aa325624c6b45b9a59812c3c0b81a5e3eb0
7c7ed1b8a8b8770e1be9c1f57f20d8549dfcbf0c1536fd52838223ebe0634629
ba28291deccc65ec836ebb6fddc78a6d3055a0a5038ba8c482b57fe23c118b81
72ccba5f360b40df9bd99450b2884b807c86a0274c5f014ed3bd0c37723d958c
1a337eda126f8acd4a41017b415ab40ce3d57a93902588cde28a175b20e30319
b6d3e9a27e92a491e1e9eee2f6d9ccaa237aeb613ae6698e1bfbe92ac2d7fdb0
7120645bacce8dd3788f10bcd73c4cb9784ad1a63e4ba47fdeb76685d94f7720
167cc6c5234be4a3646dd631f54b5c4ab139cabb6ec17d9a6de29bcabad35a8b
```

```
# HZ_2.9.0
c05310b5ee57a6f43501038599bd7ae3339db5d4a5d6d192d3abe0a75d5453a0
27cfd54b60d26b35cec236c929c6144dfaeb26625044d42a517d159ca692690b
edca3cfd7dcb6fc2abfb897de63fb2fea656662909daf4172e7b53e8d63b04f3
36d9e50c4566c33ef5a733f8e0e1c91caff39beb0309fad4962e9e83ed2a7d27
e7d9ebb6f77e57c87d80009cce9bc2699cd936984ba1a11ae3c1b9c9648616f7
26e6622a2594eec320b3a8e8ce64419875fa10012832e08ebd10fa1daaebc3fb
a9cd113410373d17d43a07196aa44c5241fb1025eda7eded2fb879ef3bd116f5
02de544313e1bc1a833b10a75c55544a0ab89aa2f370ace2581df34366d11387


# HZ_2.9.1
a26637423d6d9966b60be227e76ebe2940eb33b7c05bed1370db7bf33bca6ca3
a636a130d67d22141f1b1fad4eaf23b8cdbaf249ff2866bed526d32a344bb083
94cd891f8e4391c1d5f7cc8362661b0072f55a8f528592435752178ddcf5873e
addf28bba19123352ce84c8c0c3d5a66e084abf83bba39fa0fdd9f29011c36b8
9fa7ee1ea42aafc852ae8365de35d61230cc2e0b17ce3722aa04fc9b41682b23
28bb8c1efdd0989d8f9620168e36d7da47353e84473d39c9c08c97611d7ac615
0fcad5fd8a8ba4378fcc40028ea1db3c70fffb1c677b3ed7c26961dd303719f0
ae417734d63a46fbdf5d1959edafd0993d4292d3b3e9f938c0a13af0fbea59c5
28d86ccddda6b39f8f86beefee4ff88e37141d1d7e97683b7d17ebf31b3b6dd5
c71409c61c19f436887805a6057609557eb59dab3e59e8405bc6b20846da1489
4262b95be790d57f0e6b592e0bfd332ba031cd704d511d160be00c348242b6b7
496c6e768c20801f3658846f0367e7ddb220cb84cd6db53d6522c95bc57258ae
cfc6fcb4b0072aef491c9070761edd4b89fec0b79ec33d71800e7e6ed38f6dfc
a048aafa6380255633e7421d6db457dc799732973f81fd0bc9228320362df8d7
fa599c8c4d14783eaa8950185334f5a501123ccc6546e6836c71bfb37d2c0af6
74526152bd398ee424643d0242de63d60354acc2b453fe805250a6001a0a33c6
a918085c5c71a4beed1cf47e1ca00bb23a72a3350c5406010138e21f33ff0c9a
54fd9624a65ad212b547b4ab03a531eb9a0fed2dfe45d7e04ed63ca6d84aadee
c21ec9caf79781e0af6fa4288cbe146823a812f403eb7a2559d2cae237c86c01
efde647b19f5097b4cd0cbadac81b764b7f08a6b71172a87754f5eaee565d067
f795e0df13b946a32762b5a868ee315a7a64abb13c5ee6dd4309c529a7a3c0ad
8288d98084d63d1c0955d2393540c8638adadca7befedd5315e0cb3bd92be3fa
599aa97a88dec66247bc7c7fa56af9d40af02348b11d0145413c6a5bf81127bd
d6f568e0449d3b37956b57afbe50d03c306ffa3d03739b5a3150117f3a0ffa7d
96bbfa260f42d963aae7192350a4672c44c8a6f53f85e69c50f6be75330cc3bb
a75de07040a1964831d700ae58900c2627c2abeab0d47ca4f35b6493d2236edc
a8846d5c1f2f5ffc4e691b70ecfb52c2ca8f969bb4104af86767d70d1864d006
4bfa4436b762792f553bc8680d0c08055c664d748b518a3ae27e8d228cdab9b0
410a33a87f3b3ae2977cca9cf3d108b34470fbf3e2dd7aee8ef8257023626e63
dea438d81028ffa613e4560a4f4b629b47ff7e3430ca87be73d244ecb7410919
c847fad633ed6e33fc20e4d83344387515020bd433c82b35118eb891441556c3
ccd3c41132dfd723da71227764f6f2eb39caa63c4946076ec7c2e4b28d7bc4e6
3268ea167a491705341345dcbf621a0c3753946cbdcf27c0f7e8c95be9f99071
b4ea137b2c76086ac95cd611343a52eaf30fb88f1876abaf3e78052fc9bdff10
02055d297c81a1af042848b13984e51195dad81b70e75d0efcdffa7cbacdd74c
b1d045630bd96d6a9c3cd691f087476e421576bd7d4b1a2a122d15b73afea2af
a90e598064921b213363409fa3a1684b971cdf4d6966dbf2ea1cca6c07e9d720
b92bc3dfff4c31cc9d4eb49209202abf788934c0f039d9b336c503c3cd3dce79
```

```
9d7cbd256892ade8613645579d6e7f2a2ea9c69635a09200da2034b80c12de35
4d671ed2e3ecc2998e1d0386abc65efec88704209c1ddb791c9fcf28c2266120
d36ebb7d052c7db80705bd3dc6934ef4ef5e73d5b816d694b884ca7ffbb095a0
f27cd021ba45e3b1070a380fa6be2204cebbdf98ae6d38d90560b1f1bb6c0195
44e548e4357c177cd25326bda4c73995318d75a8262a5ab057055e41a9590e9d
8b34aa38c0fc54efc5ab45dce32e91ff8aafd818b95f456811cc06fd762e292f
6b05abbd54e10588edabad558d1537e9ae33ea53d5b9a01d140fcae59bf01c3d
5724a1b987ba86a5d6368f9dd56bdf314540a763ebdd32c6381cfbd6e5a64f78
2dafd2ad43889b2a705f2f0bf5cd12ca8e8b654d80e9dd8256374ff40822ac96
f581fbaa3fc8bfef63fd13797e0746bdd825060ab0761d2fa4d7c2ca31223740
564b5a2e9fd372f20c409dbc1b3aec5e0506f6d5584d07949e5d0f70fde6e3fd
82a54e9624d8b7570de6085c08af2916923d3c76169d3b257110bfc4501b96d5
41bf15434e1b417692edfc46395b0ca867b7af0a99f42256760c9de92d1a7d1d
e05a7f196677431b29e58a910d03fbcd8afc054c8be8ece62782e5f905a4225a
1f55c36cc81e6a4491c01a78163e5d3c1166ad2fd700fd7e3472c41d19350131
6dce40f7b700d7b2c7fc2e2d7666754a692b35268c2a79a36f6dae1704cb1cfb


# Lure documents - 7zS.sfx.exe
7740945fe6c717d3e6d0f2473cc5a69e8f027969165044597bbc959cb7f4505b
0ce39f1564d817647ebc1f8e1ed66b7df94c2fc12b1aabdd7d7f8ceb89abef87
cf0da0926e3e734813c8d7e8eaea3e1082fbfd1321aa654f21b70b2de2633ff0
4c1580ca08bca547f3458c6a6a57e17c7842f754515d0cd7112636cf9d4b1da6
bfae9c954fe53a2841a6ee5d1bae41ac746cb40ac3863afaa18446c2eca25bfc
71d9b246a961b4c5a88bca69910267c8402cf8dcc8a41c288cb6383b9fd20a30
0fe917ee75680166ced62313c2679252969cdf350313cf961933465e7e8c85c5
8c6f9a15ec399171f965c82efbda3235364264727e3a8eb65ec7e6491f5821d2
f67ffc995309c458a1490ff113b967579e61351427b9fc08c06e30f1e1a5958f
71a3143a5cd51b0fb9a04dbe1a48fd77187cb35b8765547d6698be6c76b2c07d
afa97871504f1c6f966ddaecfc53d03dcb7909d58af827f1484f4afea2ad3e1d
b080bb6cff4fad92aea207c796593b762c7f862734760f6642389ff0a2f3b073
73e58cd519d83f35d258d53b0647debef9dba13fa50c37fd92040879b2f2ebf7
adc8dd774eb2ff5416d63db4343e91790f2eb8a1b4c576c801823a07d0af0e72
43d991a52197fa8555d39f734fa32c242585b3afe5da13fa48404bde475df504
2f52f49e82a127a765c216d14196adf49850ab2080b10b66cd3eff7d2953559d
742590370b47e4fad64c9175e1c49ae3893b20c181ed7b74658eebb8c805aeff
005009f648b54788f8bbb721e2f23967fe2af90d2026e5e4119de5ebb31789a5
6188672da2b8a1d0eece3a6ac8e0a173b0d649ade5210863c953fae1638c2790
d55aaf6ab1370df0475d45db30e554c56ecad843b1792a6ad915ea447dc0079d
d1dd5e50e27d9a1f919fe639d30a6c3db96b183db8c9886fd13e77bd7d8971ea
e572e0fd2f7e21a40bd1a134f9884899cdd4e6feb263e8beb258766477555ebd
3127aa365225cb3f6c0041b938f76a87232f06b50d2119ba32c05472bba79fb6
c2bf872839700c70eadd365ee25a26203c053ed168c6db6f9443de699716bca7


# Lure documents - rtf
0b3dab65bb0881041b4c31b76ef01e94ec6969880d973b4ce6147c886558786b
74d7103af954558ed9c08b53d38c09bf32f725182375484fee17127d68a9ab56
785ae716d6c21bc923a8e1d5b79a2b230495b1356b1aa83105fa05dbf90fd0e7
8da62baadb46e347059b17f5c5b2a0be83ed6f26d0245ab41e43ad06a0f7378d
49d3b494705d8a12ea228525d875079e37f4b3f288c6348171d47d87957be408
```

```
ffef43af1d87b9e85a61aaa0c1a13bae19f9ef6b65ca3311ca9d921b53e93f86
0d8c29a3bf21564de8bc1760bc8fc9b1367b7a43c01e8ac7f6a6cdcc47f9e02b
68bc130a2e29dc9fef07cf2669e29528549ceef0207284b8bc637daa5efff9c0
791a6ba9fdfff71cc22e0a7e0a81c08b53e4aa0e9ffdb429851f7df09bf3aed8
10f3b8ae627e719320def4cfa77f174f5a03b42192da27628ef17a3499f860bf
1a6062a97efc0d08c6198d0ec0ad84fa74e7b18422b2c1e05762a5c25793a46b
40c0b6b59272d8b458c4a10159572e2dbfc932991eb7d294b74ec6e1af2f6f8d
9dc4d8eb8243e48218668dbfc4565a893e74a25c23d2bb38b720a282c24fbe02
0ab18cf4dc2292f9cb6e56f7db2b3c8dd782e4e9343f49a67f44e0015fafdd17
cd0aeaa018ad11e56de0e53f8c13df4e1ffe30e4ac2b3bc2e11851c2789b708d
0a0964b33576a8e99a0c7e83034ccdca7e6b1062a3cf47fec002a47b27b3a431
b3684ae83329777d7d560e88f16fb8cccc34245bd47e624412749048e861db4f
5d10626def63b4c2c0751a7a745e097a33d8a24e84855eecd4ff01048c0b11d2
05e90bfeddbe5ba92e9d8c486728f74be4b3f0ab6050af38163d675cc067219d
fa40ac3d37f98d19e2e3a850a753a6ff68ad884a8fbc598feaf460f2854782ad
355f251f272603bb08cb97ca48dcdf3e30f5d33013e5fefbb35442baee87550e
6941e8a0bce0425597e7de0626466eaf44700dafdaa602165c321f3ffab68899
e73444fe6116d5875630ede150c33fb4fe5fd538288b021d6d271f2622f7771b
9871526350bbf79a6c1884e1644087137cd874e401b6c5182ecf6ddd9a229aea
c90c0dfcba9219b3e1923bac0b11e241482d2f260ef667a611e61af07f1f4319
9a758307569dbd60913f2b710bbe0b2948dedd9c49a077aa584591b4a4ba49f7
dc84392afac92536dc25e351032635f08c8cad3a8356d19d0f39f3873e00da4b
670c87a77a327e0f9558931e2b4c9d2e892220d28ab4e81ecf15fea3d4d2a7e8
6a7e26f57b6fb0b294ce689f822de935b8204c07e7442dd05b5d101da1df442b
7cd1b1fa4fb1feb80c2ab809544b80e99b717b6c6f1720a4b586fe17358dd333
8d85e178732398fe6dff67716879c957fc13a0aac6366340f7d21a635b50516a
7b3c52a8422ad139627ac1bd2402d259f256863e253f1ee177579148a0820e53
35dd7275391128218e1280e1be04c4508b43055f9b6e35f3999c1bf2506ac824



# Cobalt Strike
15a3175f0097386f617c33fb2552dc8e5972055bb4ff99ef8532763e248543b7
40b46a3d38c80a4bb4a2b0a3eeaa6e420ff6d180a51f43121955ca1a05695b05
41371f62de279d71243adc0e7dd7576007c2c4facff16def41c82fe638cb6fbe
c9777c64231161b8e3d941d6ea37d081c12cef830cbdf92fcb245a8f29ccd8e0
5801b9c635f36eb82f154e3c349bfc30724c4f3334ef8ea1e5fa20b5d022592b
d4fa8743874c2c1c3b2b643f54470a5d2f72a7a400a04cd7e36f5ee6ad7a907b
94b0bda42e7d1e01bf0b832742526d1975c7f211440c646c54ef58c5d7a8fa06
e83be4a374a989296bb511167ec20361454b758f5b001ea4f03393b1b56669d9



# Cobalt Strike pdb path
C:\Users\dell\source\repos\WindowsProject1\Debug\WindowsProject1.pdb
C:\Users\dell\source\repos\WindowsProject2\Release\WindowsProject2.pdb



# C2 server - Cobalt Strike
81.68.122[.]239
hxxp://81[.]68.122.239:443/1Pfu
hxxp://81[.]68.122.239/Rbs5
```

```
# C2 server - HZ
Rat101[.]114.114.114:9002106[.]120.215.202:8089106[.]52.119.45:8081107[.]175.172.101:8
 # oa.pumch.cn115[.]236.55.14:11111116[.]236.40.57:8081 #
finance.yto.net.cn116[.]54.125.202:8081116[.]6.102.21:8081116[.]6.102.24:8081123[.]60.
 # www.hbzyjxkh.cn, hbszyy.gcptrial.com,
zhyy.hbszyy.cn183[.]196.83.220:8081183[.]6.106.176:8877183[.]6.50.76:8081185[.]185.185
 #
dsm.hn.sgcc.com.cn219[.]238.141.242:8081220[.]168.209.150:8081220[.]248.243.82:8081220
 #
sgwpdm.ah.sgcc.com.cn221[.]195.106.200:8081221[.]195.106.200:9090222[.]85.157.82:80813
```

MITRE ATT&CK

```
T1003       Credential DumpingT1041       Exfiltration Over C2 ChannelT1012
Query RegistryT1082       System Information DiscoveryT1112       Modify
RegistryT1203       Exploitation for Client ExecutionT1204.002   Malicious FileT1204
User ExecutionT1566.001   Spearphishing AttachmentT1566       Phishing
```

Yara rule

```
rule hz_rat
{
  strings:
      $x_mutex = "91E99696-92CC-43F4-99B0-774D80BDAA6B"
      $x_pdb_path_2_8_2__and_2_9_0 = "D:\\WORKSPACE\\HZ_"
      $x_pdb_path_2_9_1  = "D:\\WORKSPACE\\HP\\HZ_"
      $x_pdf_path
="C:\\Users\\dell\\source\\repos\\WindowsProject2\\Release\\WindowsProject1.pdb"
      $x_pdb_path_short_part = "hp_client_win"
      $x_wrongly_written_error_msg = "instanse already exist."
  condition:
      any of them
}



rule hz_rat_aes_packer
{
 strings:
    $decryption_body_747 = { 8D 44 24 1C 89 04 24 E8 84 ED 00 00 E8 DF DE 00 00 C7 44
24 08 10 00 00 00 C7 44 24 04 20 30 41 00 8D 44 24 54 89 04 24 C7 44 24 20 01 00 00
00 E8 B7 00 00 00 C7 84 24 3C 02 00 00 00 00 00 C7 84 24 38 02 00 00 00 00 00
EB 4B 8B 84 24 38 02 00 00 C1 E0 04 8D 90 40 30 41 00 8B 84 24 38 02 00 00 C1 E0 04
05 40 30 41 00 89 54 24 08 89 44 24 04 8D 44 24 54 89 04 24 C7 44 24 20 01 00 00 00
E8 E9 0E 00 00 83 84 24 3C 02 00 00 10 83 84 24 38 02 00 00 01 81 BC 24 3C 02 00 00
?? ?? ?? 00 76 A8 B8 40 30 41 00 C7 44 24 20 01 00 00 00 FF D0 B8 00 00 00 00 89 44
24 18 EB 14 8B }
    $decryption_body_748 = { 55 89 E5 5D C3 90 90 90 90 90 90 90 90 90 90 90 8D 4C 24
04 83 E4 F0 FF 71 FC 55 89 E5 57 56 53 51 81 EC 68 02 00 00 C7 85 CC FD FF FF 80 24
41 00 C7 85 D0 FD FF FF 3C 2B 41 00 8D 85 D4 FD FF FF 8D 4D E8 89 08 BA 28 17 40 00
89 50 04 89 60 08 8D 85 B4 FD FF FF 89 04 24 E8 51 EE 00 00 E8 AC DF 00 00 C7 44 24
08 10 00 00 00 C7 44 24 04 20 30 41 00 8D 85 F0 FD FF FF 89 04 24 C7 85 B8 FD FF FF
01 00 00 00 E8 78 01 00 00 C7 45 E4 00 00 00 00 C7 45 E0 00 00 00 00 EB 3F 8B 45 E0
C1 E0 04 8D 90 40 30 41 00 8B 45 E0 C1 E0 04 05 40 30 41 00 89 54 24 08 89 44 24 04
8D 85 F0 FD FF FF 89 04 24 C7 85 B8 FD FF FF 01 00 00 00 E8 B6 0F 00 00 83 45 E4 10
83 45 E0 01 81 7D E4 ?? ?? ?? 00 76 B8 A1 5C 71 45 00 C7 85 B8 FD FF FF 01 }

 condition:    any of them}
```

One more thing …

Reaching the end of our analysis, we noticed that many C2 servers we previously identified provide current or even unknown samples of HZ Rat.

The samples are provided in general under the following path pattern:

```
<C2-Server-IP>:<C2-Server-PORT>/<original_sample_name>
```

Based on this pattern, we identified the following servers providing HZ Rat for download:

```
# C2 server urls providing HZ
Rat:106[.]120.215.202:8089/default.exe114[.]113.238.83:9000/default.exe114[.]113.238.8
 #
oa.pumch.cn116[.]54.125.202:8081/default.exe116[.]6.102.21:8081/default.exe124[.]250.1
 #
sgwpdm.ah.sgcc.com.cn222[.]85.157.82:8081/default.exe58[.]240.32.125:8081/default.exe6
 #
finance.yto.net.cn220[.]250.20.68:8081/winIogon.exe218[.]65.110.180:8081/winIogon.exe2
```

Picture of us heavily uploading HZ Rat samples fresh from C2 server to VirusTotal.