PikaBot

Published: 2023-02-26 · Archived: 2026-04-05 14:21:34 UTC

```
stack_strings = [{'start': 5902456, 'end': 5902507, 'op_offset': -48}, {'start': 5902507, 'end': 590

def emulate(start, end, op_offset):
    dp = Dumpulator("/tmp/pika2.dmp", quiet=True)
    print('loaded')
    dp.start(start, end=end)
    print('done')
    str_len = dp.regs.ecx
    if str_len > 2:
        if dp.read(dp.regs.ebp + op_offset, 2)[1] == 0:
            out = dp.read(dp.regs.ebp + op_offset, str_len * 2)
            out = out.replace(b'\x00',b'')
        else:
            out = dp.read(dp.regs.ebp + op_offset, str_len)
    else:
        out = dp.read(dp.regs.ebp + op_offset, str_len)
    return out


labels = {}
for ss in stack_strings:
    try:
        out = emulate(ss.get('start'), ss.get('end'),ss.get('op_offset'))
        if out.isascii():
            print(f"{hex(ss.get('start'))}: {out.decode('utf-8')}")
            labels[ss.get('start')] = out.decode('utf-8')
        else:
            print(f"ERROR: {hex(ss.get('start'))}: {out}")

    except:
        print(f"TOTAL FAILURE:  {hex(ss.get('start'))}")


print(labels)
```

```
loaded
done
0x5a1078: RegOpenKeyExW
loaded
```

```
done
0x5a10ab: HARDWARE\ACPI\DSDT\VBOX__
loaded
done
0x5a113b: GetUserDefaultLangID
loaded
done
0x5a11c9: CreateMutexW
loaded
done
0x5a1203: {8B30B3CD-2068-4F75-AB1F-FCAE6AF928B6}
loaded
done
0x5a1287: GetLastError
loaded
done
0x5a12cb: wsprintfW
loaded
done
0x5a12f8: SOFTWARE\%s
loaded
done
ERROR: 0x5a132f: bytearray(b'\x05\x06\x05\t\xfc\n\n\x0b\xf8\x05\x0b\xe6\x0c\x0b\x03\r\xfc\n\xdb\xfa\
loaded
done
0x5a1398: RegCreateKeyExW
loaded
done
0x5a13d5: wsprintfW
loaded
done
0x5a1402: schtasks.exe /Create /F /TN "%s" /TR " cmd /q /c start /min \"\" powershell \"$%s = Get-It
loaded
done
0x5a164b: {8B30B3CD-2068-4F75-AB1F-FCAE6AF928B6}
loaded
done
ERROR: 0x5a16d4: bytearray(b'\x00\x81\x00\x81\x00\x81\x08\x81H\x80\x08\x81\x00\x81\x08\x81\x08\x81H\
loaded
done
0x5a173e:
loaded
done
ERROR: 0x5a17a0: bytearray(b'\x00\x80\x00\x80\x00\x80\x08\x80H\x81\x08\x80\x00\x80\x08\x80\x08\x80H\
loaded
done
0x5a180b: @@H@HHH@H@HH@@@@H
```

```
loaded
done
0x5a185b:
loaded
done
0x5a1888: GetModuleFileNameW
loaded
done
0x5a18c4: wsprintfW
loaded
done
0x5a18fc: @H@H@@HH@HH@@HHH@@@@@@
loaded
done
0x5a199f: CreateProcessW
loaded
done
0x5a1aac: RegSetValueExW
loaded
done
0x5a1aee:
loaded
done
0x5a1bcc: RegCloseKey
loaded
done
0x5a1d93: CreateProcessW
loaded
initial unmapped read from 8df790[1], cip = 5a1dce, exception: ExceptionType.Memory, (0x5a1dce, 0x2d
final unmapped read from 8df790[1], cip = 5a1deb, exception: ExceptionType.Memory, (0x5a1deb, 0x10, (
```

```
Traceback (most recent call last):
  File "/Users/herrcore/.pyenv/versions/3.9.5/lib/python3.9/site-packages/dumpulator/dumpulator.py",
    status = syscall_impl(dp, *args)
  File "/Users/herrcore/.pyenv/versions/3.9.5/lib/python3.9/site-packages/dumpulator/ntsyscalls.py",
    raise NotImplementedError()
NotImplementedError
```

```
Exception thrown during syscall implementation, stopping emulation!
forced exit memory operation 21 of 4fe2[1] = 0
TOTAL FAILURE:  0x5a1dce
loaded
initial unmapped read from 8df790[1], cip = 5a1dfb, exception: ExceptionType.Memory, (0x5a1dfb, 0x2d
final unmapped read from 8df790[1], cip = 5a1e18, exception: ExceptionType.Memory, (0x5a1e18, 0x10, (
```

```
Traceback (most recent call last):
  File "/Users/herrcore/.pyenv/versions/3.9.5/lib/python3.9/site-packages/dumpulator/dumpulator.py",
    status = syscall_impl(dp, *args)
  File "/Users/herrcore/.pyenv/versions/3.9.5/lib/python3.9/site-packages/dumpulator/ntsyscalls.py",
    raise NotImplementedError()
NotImplementedError
```

```
Exception thrown during syscall implementation, stopping emulation!
forced exit memory operation 21 of 4fe2[1] = 0
TOTAL FAILURE:  0x5a1dfb
loaded
done
0x5a2013: Kernel32.dll
loaded
done
0x5a2041: User32.dll
loaded
done
0x5a2075: Advapi32.dll
{5902456: 'RegOpenKeyExW', 5902507: 'HARDWARE\\ACPI\\DSDT\\VBOX__', 5902651: 'GetUserDefaultLangID',
```

Source: https://research.openanalysis.net/pikabot/yara/config/loader/2023/02/26/pikabot.html