yaralab
www.yaralab.eu

YARA, az információbiztonság svájci bicskája

Dr. Leitold Ferenc
Veszprog Kft.
fleitold@veszprog.hu

Tartalom

yaralab
www.yaralab.eu

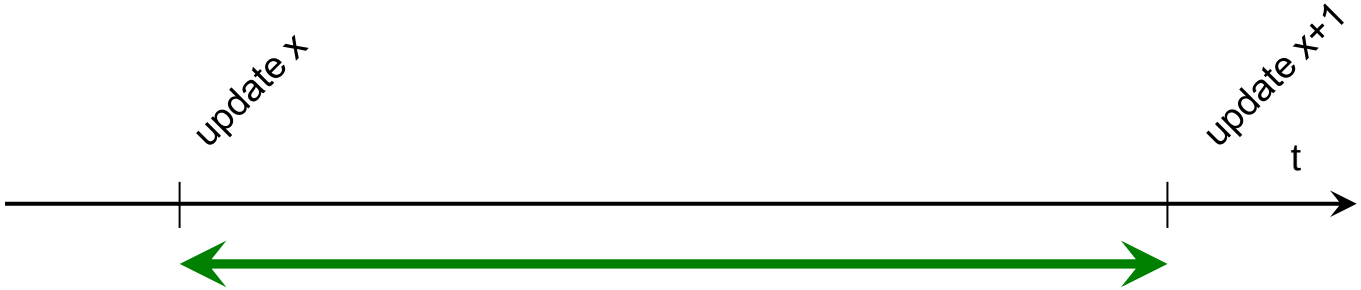
- Történeti áttekintés
- Mi is az a YARA?
- Miért előnyös a YARA használata?
- Mi szükséges a YARA használatához?
- Mennyire hatékony a YARA?

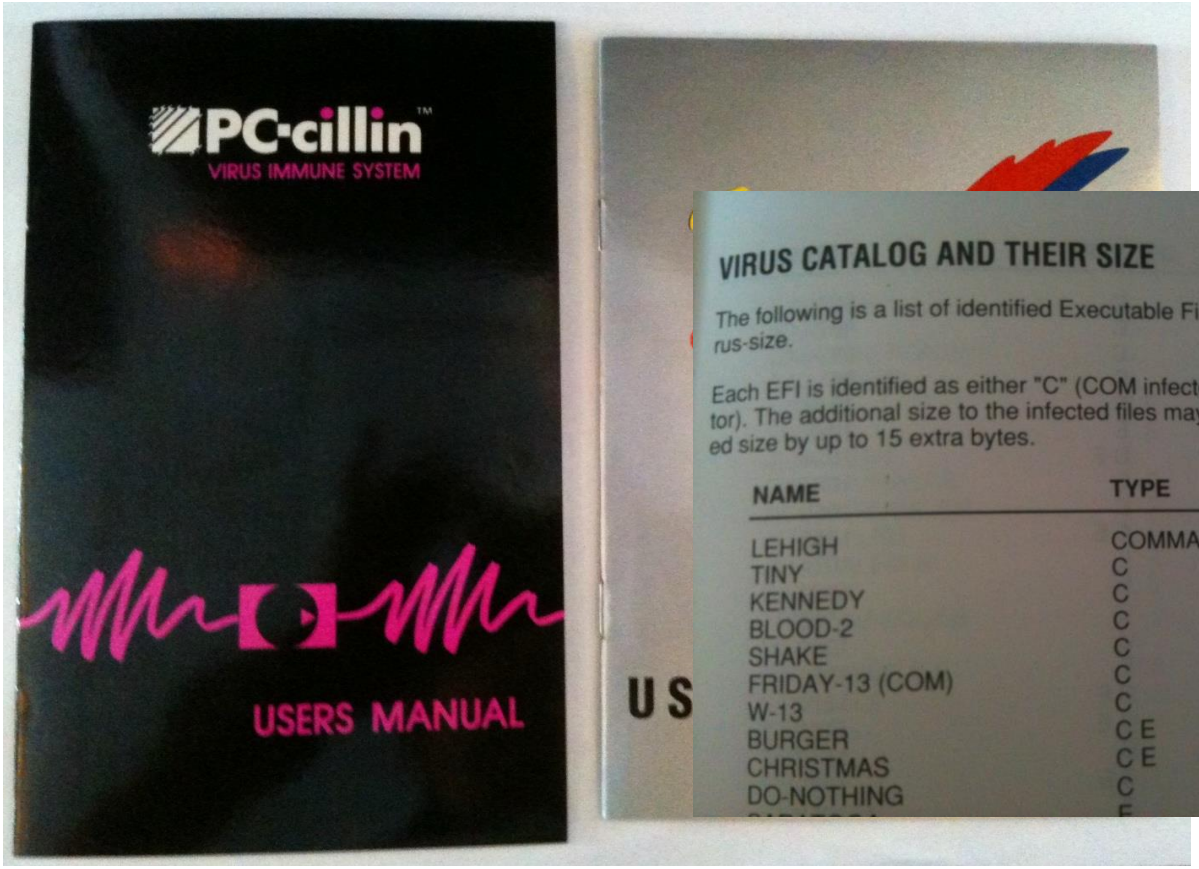
Védelmek frissítései

yaralab
www.yaralab.eu

1990

Frissítések
havonta/negyedévente





VIRUS CATALOG AND THEIR SIZE

The following is a list of identified Executable File Infector (EFI), sorted by virus-size.

Each EFI is identified as either "C" (COM infector) and/or "E" (EXE file infector). The additional size to the infected files may sometimes exceed the quoted size by up to 15 extra bytes.

NAME	TYPE	ADD SIZE
LEHIGH	COMMAND	0
TINY	C	163
KENNEDY	C	308
BLOOD-2	C	427
SHAKE	C	476
FRIDAY-13 (COM)	C	512
W-13	C	532
BURGER	C E	560
CHRISTMAS	C E	600
DO-NOTHING	C	608
	E	632

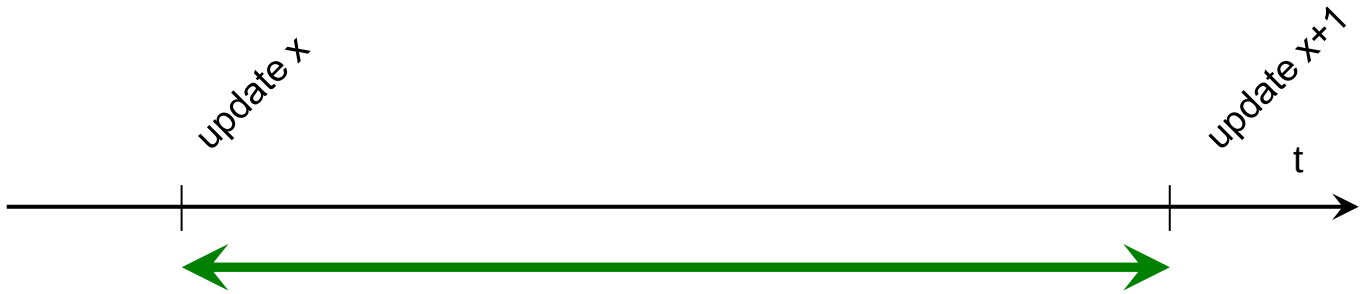
105
vírus
listája

Védelmek frissítései

yaralab
www.yaralab.eu

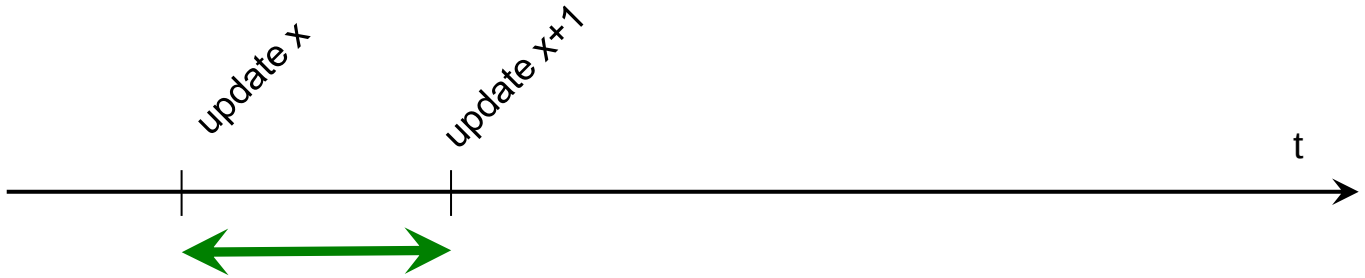
1990

Frissítések
havonta/negyedévente



2000

Frissítések
naponta

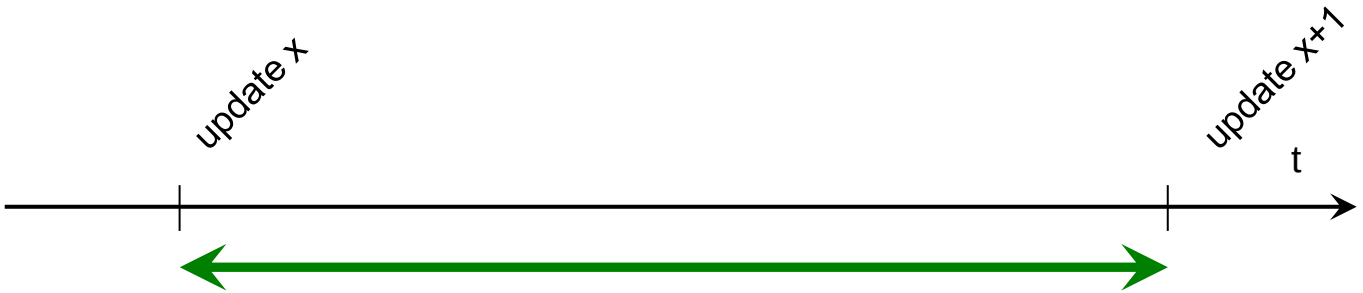


Védelmek frissítései

yaralab
www.yaralab.eu

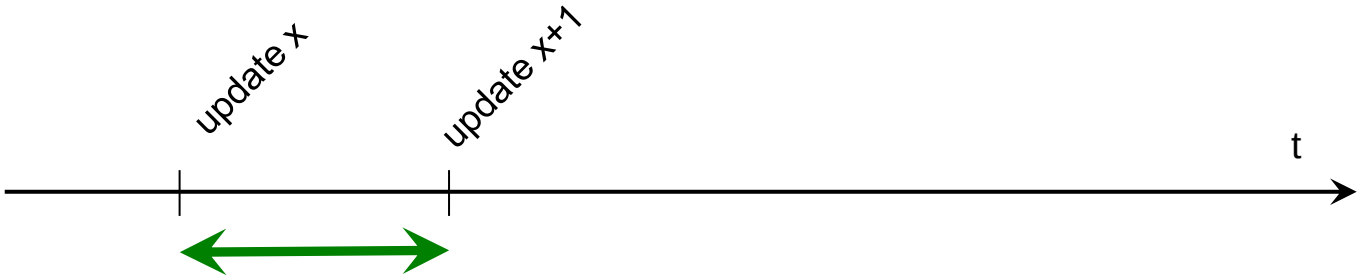
1990

Frissítések
havonta/negyedévente



2000

Frissítések
naponta



2010

Felhő használata

Felhő alapú biztonság

yaralab
www.yaralab.eu

Trend Micro
Smart Protection Network
Tuesday, 14 Sep. 2010

E-mail ellenőrzések
6.2 milliárd
E-mail blokkolások
4.4 milliárd

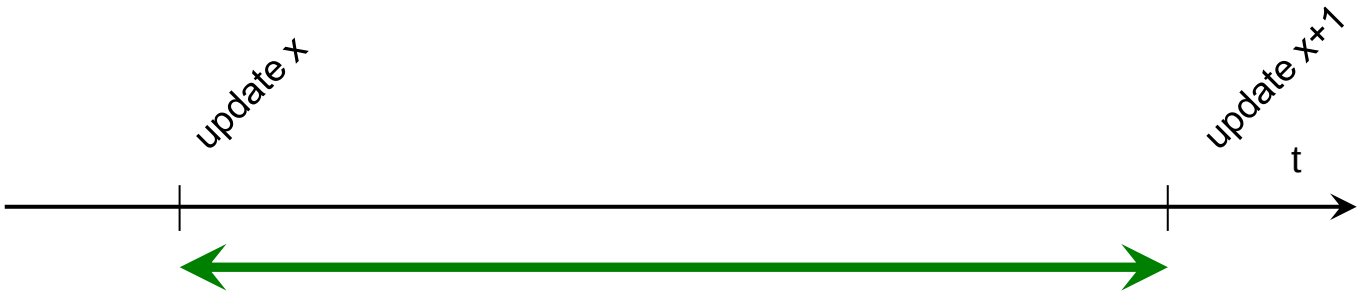
Webcím ellenőrzések
41 milliárd
Webcím blokkolások
585 millió

Védelmek frissítései

yaralab
www.yaralab.eu

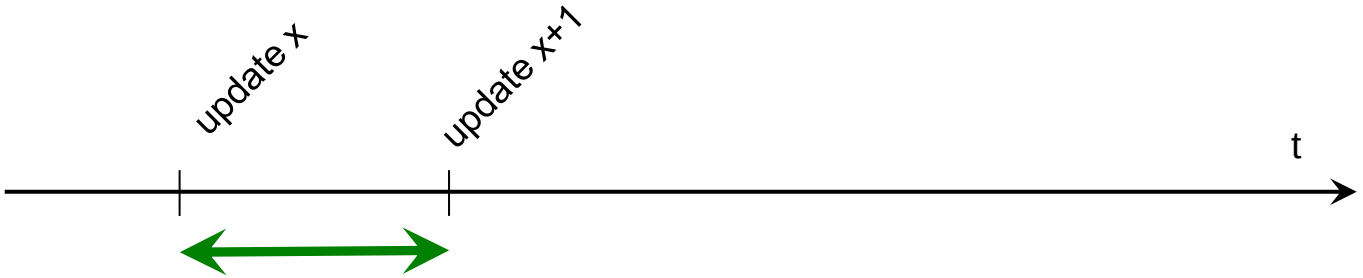
1990

Frissítések
havonta/negyedévente



2000

Frissítések
naponta



2010

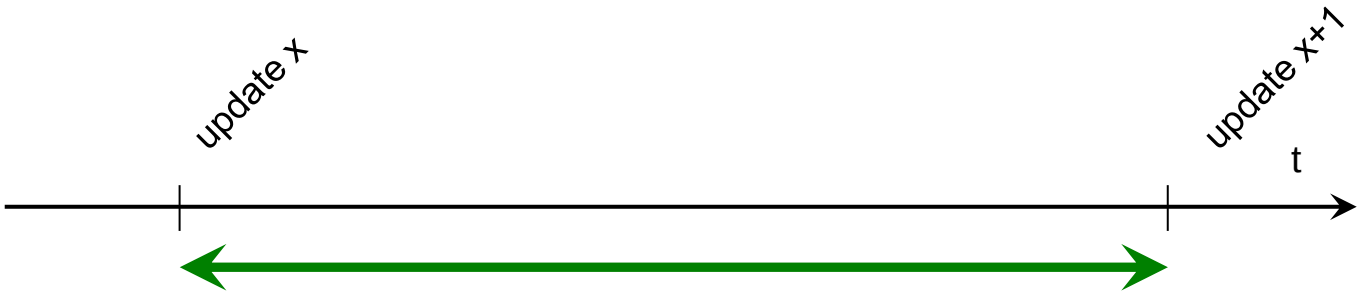
Felhő használata

Védelmek frissítései

yaralab
www.yaralab.eu

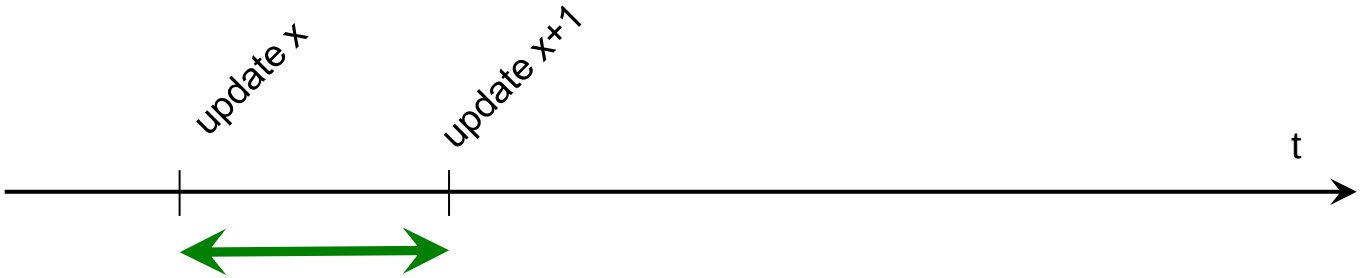
1990

Frissítések
havonta/negyedévente



2000

Frissítések
naponta



2010

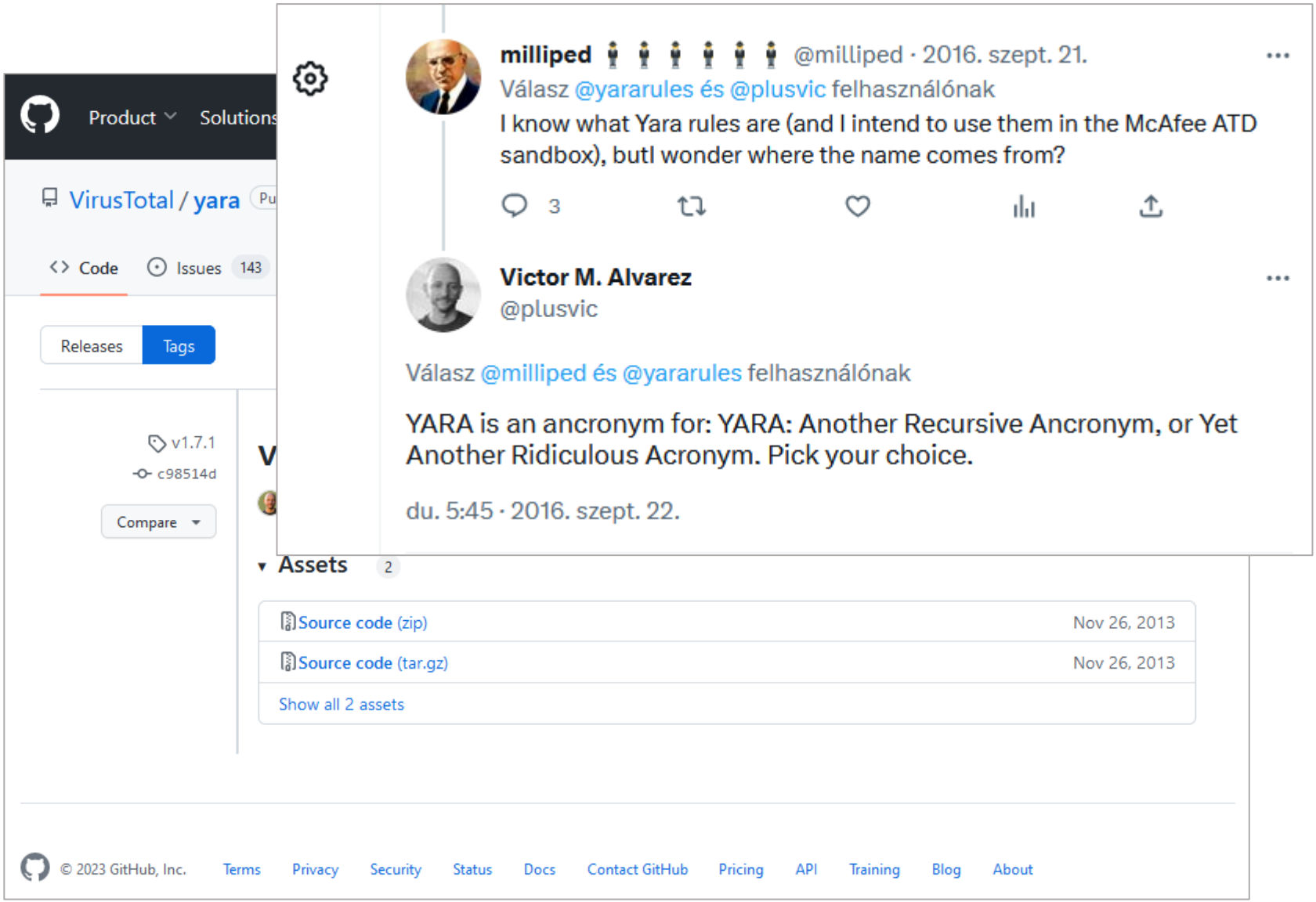
Felhő használata

2020

Veszélyforrások gyártótól független kezelése: SOC + **YARA**

A YARA eredete

yaralab
www.yaralab.eu



YARA szabály

yaralab
www.yaralab.eu

```
rule dummy
{
      meta:
         $meta_string = “dummy rule“
         $meta_version = 4
         $meta_valid = true
      strings:
         $text_string = "text here"
      condition:
         $text_string
}
```

YARA szabály

yaralab
www.yaralab.eu

```
rule dummy
{
      meta:
         $meta_string = “dummy rule“
         $meta_version = 4
         $meta_valid = true
      strings:
         $text_string = "text here"
      condition:
         $text_string
}
```

YARA szabály

yaralab
www.yaralab.eu

```
rule dummy
{
      meta:
         $meta_string = “dummy rule“
         $meta_version = 4
         $meta_valid = true
      strings:
         $text_string = "text here"
      condition:
         $text_string
}
```

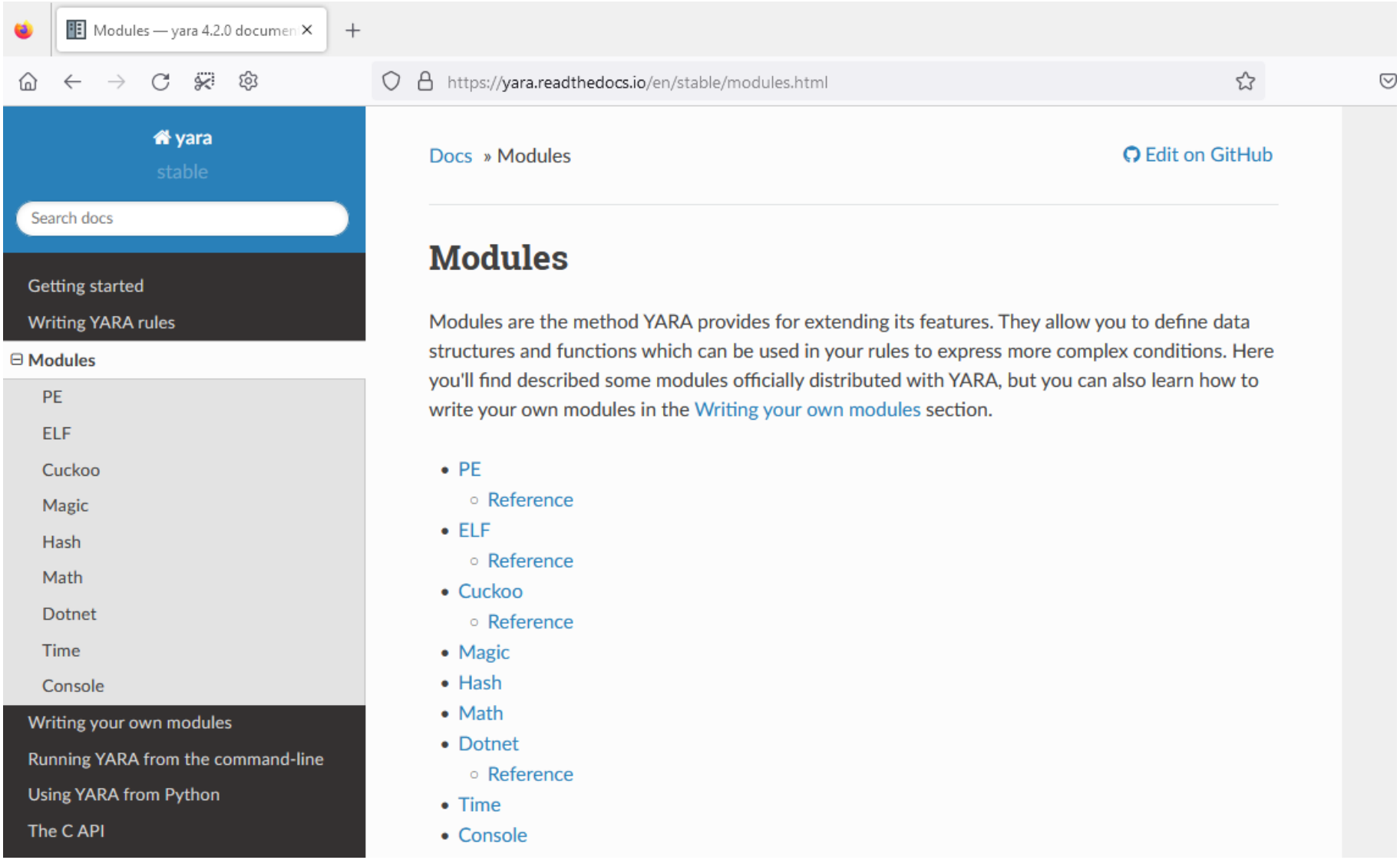
YARA szabály

yaralab
www.yaralab.eu

```
rule dummy
{
    meta:
        $meta_string = “dummy rule“
        $meta_version = 4
        $meta_valid = true
    strings:
        $text_string = "text here"
    condition:
        $text_string
}
```

YARA modulok

yaralab
www.yaralab.eu



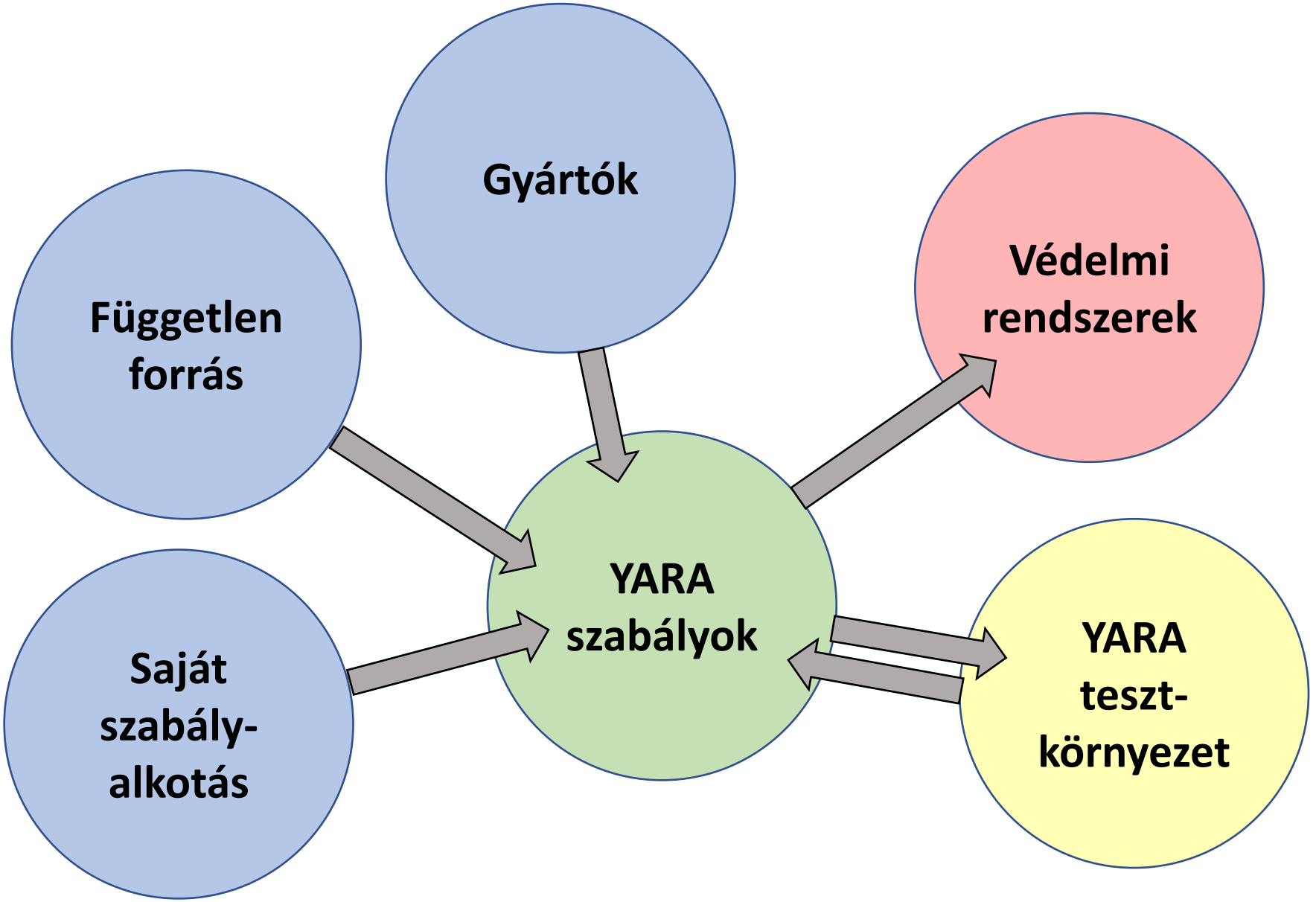
A YARA előnyei

yaralab
www.yaralab.eu

- Saját keresési szabályok
  - -> gyorsaság
  - -> vaklármák kezelése
- Külső YARA szolgáltatók
  - -> gyártótól független keresési algoritmusok
- Különböző védelmi rendszerek azonos keresési algoritmusokkal

YARA használata

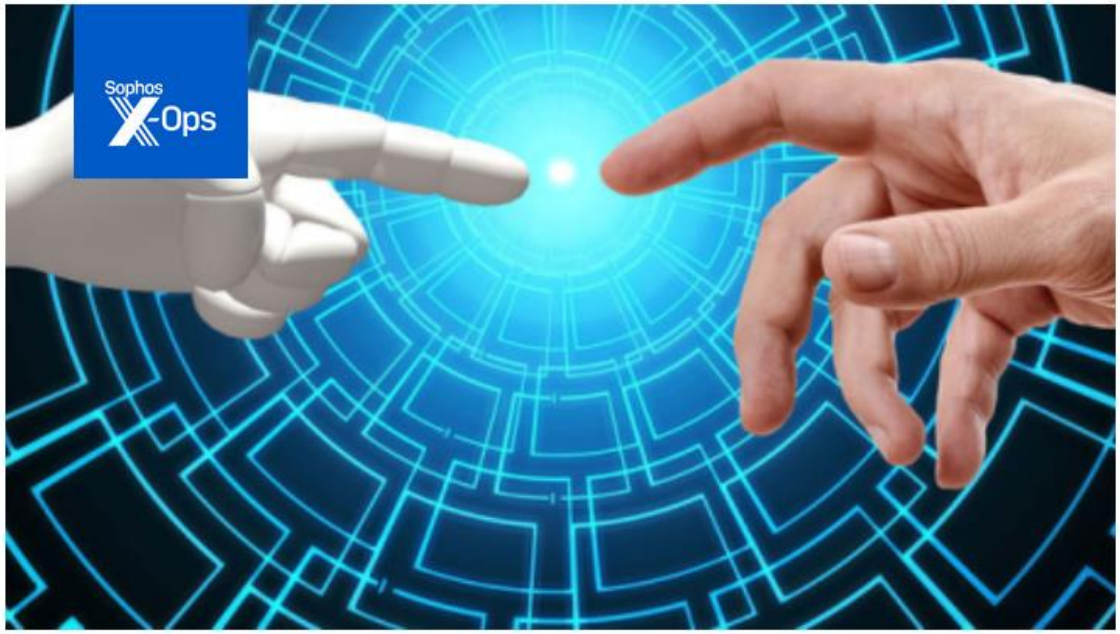
yaralab
www.yaralab.eu



Mennyire hatékony a YARA?

yaralab
www.yaralab.eu

SOPHOS NEWS | Products & Services | Security Operations | Threat Research | AI Research | Security News | Sophos Life



An open-source ML toolkit for automatically generating YARA rules

The SophosAI Artificial Intelligence team has developed a machine-learning based tool that generates YARA rules for detecting specific types of threats

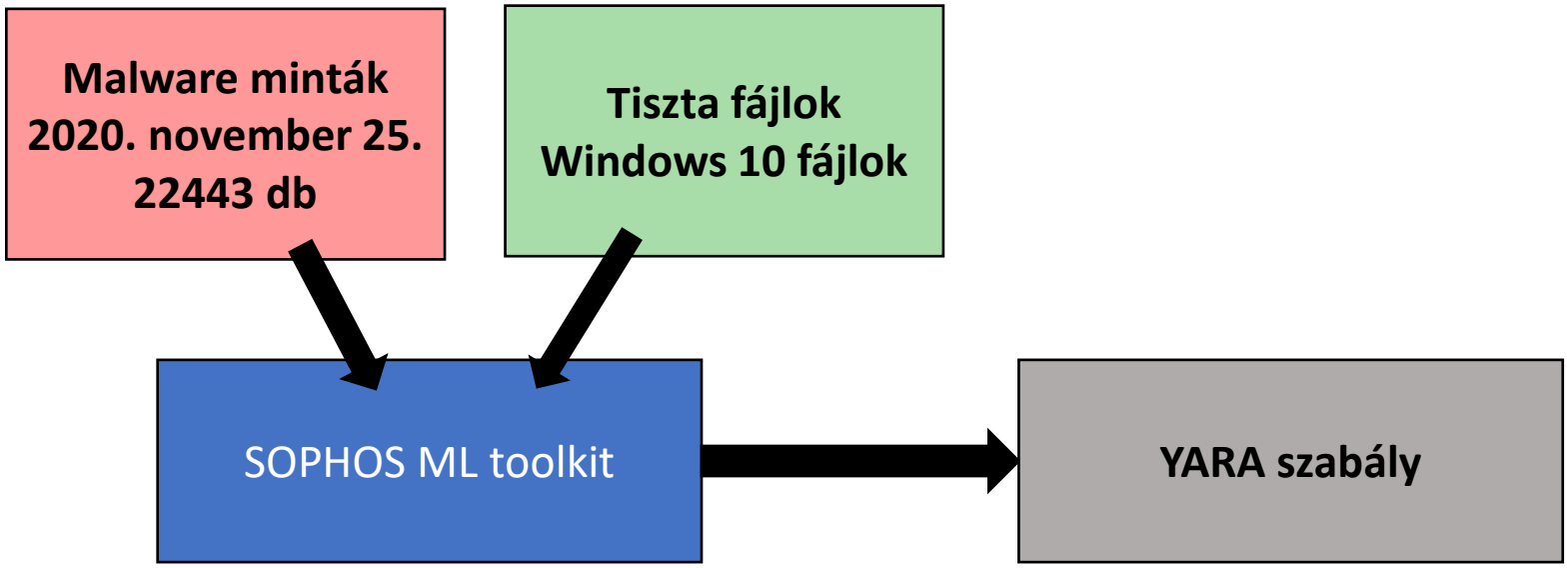
Written by Sean Gallagher

AUGUST 25, 2022

AI RESEARCH | FREE TOOLS | INCIDENT RESPONSE TOOLS | OPEN SOURCE | SECURITY OPERATIONS | THREAT HUNTING TOOLS

Mennyire hatékony a YARA?

yaralab
www.yaralab.eu



Mennyire hatékony a YARA?

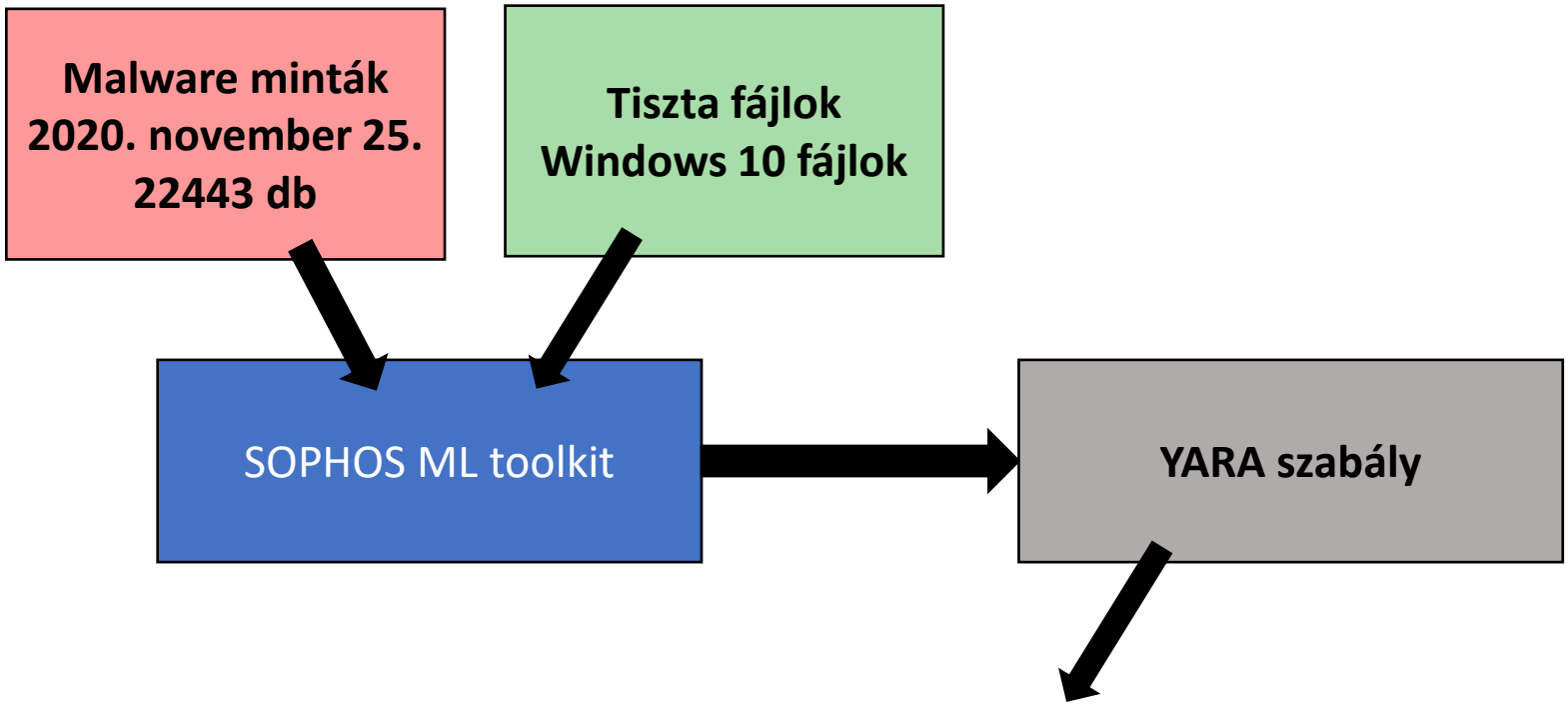
yaralab
www.yaralab.eu

```
/data/yaratest/rules/1/ml-rule-t1-1.yara
rule ml1
{
    strings:
        $s0 = "RtlLookupFunctionEntry" fullword // weight: 5.328
        $s1 = "RtlVirtualUnwind"   fullword // weight: 3.967
        $s2 = "GetModuleHandleA"   fullword // weight: 2.938
        $s3 = "CompilationRelaxationsAttribute" fullword // weight: 2.794
        $s4 = "IQRerSPOLogHcPd3bO" fullword // weight: 2.554
        $s5 = "InterlockedExchange" fullword // weight: 2.468
        $s6 = "IOleInPlaceUIWindow" fullword // weight: 2.362
        $s7 = "rrrrrrrrrrrrrrrrrrrrrrrrrrrrrr9999" fullword // weight: 2.227
        $s8 = "vbaExceptHandler"   fullword // weight: 2.198
        $s9 = "WNetEnumResourceA"  fullword // weight: 2.129
        $s10 = "giiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiJkMkKkkkkkkknnn" fullword // weight: 1.966
        $s11 = "abcdefghijklmnopq"  fullword // weight: 1.928
        $s12 = "AVCacheLocalScheduleGroupSegment" fullword // weight: 1.908
        $s13 = "IsDebuggerPresent"  fullword // weight: 1.858
        $s14 = "InterlockedCompareExchange" fullword // weight: 1.747
        $s15 = "CertCompareCertificateName" fullword // weight: 1.628
        $s16 = "GetEnvironmentVariableW" fullword // weight: 1.413
        $s17 = "InitializeSListHead" fullword // weight: 1.392
        $s18 = "GetEnvironmentStringsA" fullword // weight: 1.29
        $s19 = "717A7Q7a7q77777777" fullword // weight: 1.221
        $s20 = "GetLongPathNameW"   fullword // weight: 1.143
        $s21 = "USERTrustRSACertificationAuthority" fullword // weight: 1.133
        $s236 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" fullword // weight: -2.914
        $s237 = "TraceRegisterExA"   fullword // weight: -3.421
        $s238 = "LdrDisableThreadCalloutsForDll" fullword // weight: -3.52
        $s239 = "qRqRqRepRePpRRichqR" fullword // weight: -6.123
        $s240 = "KbdLayerDescriptor" fullword // weight: -7.009

    condition:
        ((#s0 * 5.328) + (#s1 * 3.967) + (#s2 * 2.938) + (#s3 * 2.794) + (#s4 * 2.554) + (#s5 * 2.468) + (#s6 * 2.362) + (#s7 * 2.227) + (#s
0 * 1.966) + (#s11 * 1.928) + (#s12 * 1.908) + (#s13 * 1.858) + (#s14 * 1.747) + (#s15 * 1.628) + (#s16 * 1.413) + (#s17 * 1.392) + (#s18 *
 1.143) + (#s21 * 1.133) + (#s22 * 0.937) + (#s23 * 0.905) + (#s24 * 0.882) + (#s25 * 0.764) + (#s26 * 0.749) + (#s27 * 0.648) + (#s28 * 0.5
569) + (#s31 * 0.562) + (#s32 * 0.560) + (#s33 * 0.530) + (#s34 * 0.529) + (#s35 * 0.529) + (#s36 * 0.528) + (#s37 * 0.522) + (#s38 * 0.504)
) + (#s41 * 0.491) + (#s42 * 0.487) + (#s43 * 0.483) + (#s44 * 0.459) + (#s45 * 0.408) + (#s46 * 0.380) + (#s47 * 0.378) + (#s48 * 0.365) +
 (#s51 * 0.295) + (#s52 * 0.283) + (#s53 * 0.256) + (#s54 * 0.242) + (#s55 * 0.228) + (#s56 * 0.225) + (#s57 * 0.218) + (#s58 * 0.217) + (#s
s61 * 0.204) + (#s62 * 0.193) + (#s63 * 0.187) + (#s64 * 0.164) + (#s65 * 0.161) + (#s66 * 0.153) + (#s67 * 0.152) + (#s68 * 0.148) + (#s69
 * 0.127) + (#s72 * 0.117) + (#s73 * 0.117) + (#s74 * 0.114) + (#s75 * 0.113) + (#s76 * 0.111) + (#s77 * 0.094) + (#s78 * 0.090) + (#s79 * 0
0.076) + (#s82 * 0.073) + (#s83 * 0.070) + (#s84 * 0.070) + (#s85 * 0.067) + (#s86 * 0.065) + (#s87 * 0.051) + (#s88 * 0.048) + (#s89 * 0.04
35) + (#s92 * 0.034) + (#s93 * 0.029) + (#s94 * 0.027) + (#s95 * 0.023) + (#s96 * 0.022) + (#s97 * 0.020) + (#s98 * 0.015) + (#s99 * 0.014)
2) + (#s102 * 0.008) + (#s103 * 0.007) + (#s104 * 0.007) + (#s105 * 0.007) + (#s106 * 0.002) + (#s107 * -0.002) + (#s108 * -0.003) + (#s109
s111 * -0.009) + (#s112 * -0.009) + (#s113 * -0.014) + (#s114 * -0.017) + (#s115 * -0.018) + (#s116 * -0.021) + (#s117 * -0.024) + (#s118 *
20 * -0.038) + (#s121 * -0.039) + (#s122 * -0.039) + (#s123 * -0.040) + (#s124 * -0.040) + (#s125 * -0.046) + (#s126 * -0.056) + (#s127 * -0
 * -0.098) + (#s130 * -0.104) + (#s131 * -0.109) + (#s132 * -0.134) + (#s133 * -0.138) + (#s134 * -0.158) + (#s135 * -0.160) + (#s136 * -0.1
 -0.179) + (#s139 * -0.190) + (#s140 * -0.190) + (#s141 * -0.191) + (#s142 * -0.196) + (#s143 * -0.198) + (#s144 * -0.204) + (#s145 * -0.208
0.212) + (#s148 * -0.222) + (#s149 * -0.239) + (#s150 * -0.241) + (#s151 * -0.242) + (#s152 * -0.258) + (#s153 * -0.263) + (#s154 * -0.288)
324) + (#s157 * -0.331) + (#s158 * -0.332) + (#s159 * -0.339) + (#s160 * -0.341) + (#s161 * -0.341) + (#s162 * -0.342) + (#s163 * -0.351) +
6) + (#s166 * -0.386) + (#s167 * -0.386) + (#s168 * -0.402) + (#s169 * -0.411) + (#s170 * -0.411) + (#s171 * -0.427) + (#s172 * -0.430) + (#
```

Mennyire hatékony a YARA?

yaralab
www.yaralab.eu



Malware minták – 2023. március 8-17:
(>98% 2023-as felbukkanású)

91,45% - 96,25%

Windows fájlok:

0,33%

További részletek: www.yaralab.eu

yaralab
www.yaralab.eu