



# YARA, az információbiztonság svájci bicskája

*Dr. Leitold Ferenc*  
*Veszprog Kft.*  
[fleitold@veszprog.hu](mailto:fleitold@veszprog.hu)

# Tartalom

 Történeti áttekintés

 Mi is az a YARA?

 Miért előnyös a YARA használata?

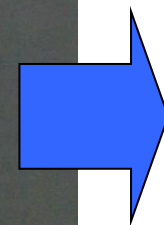
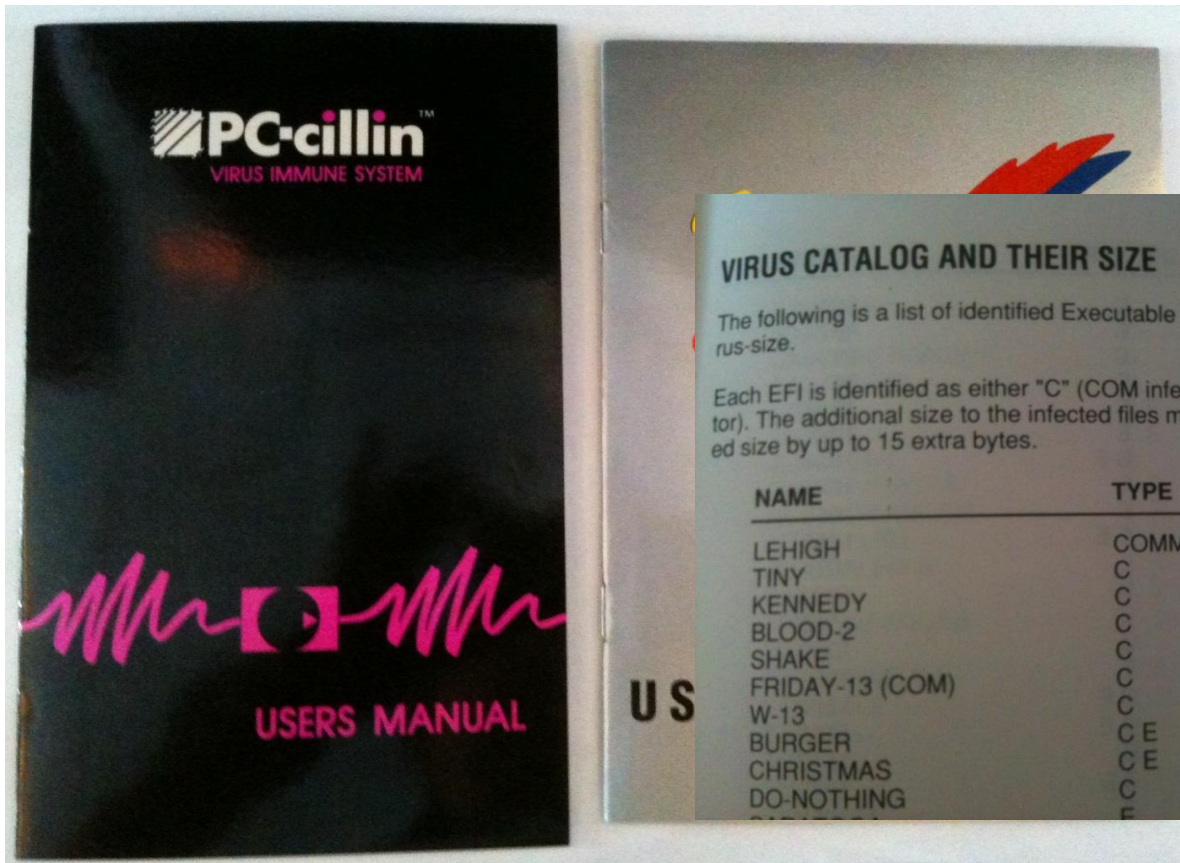
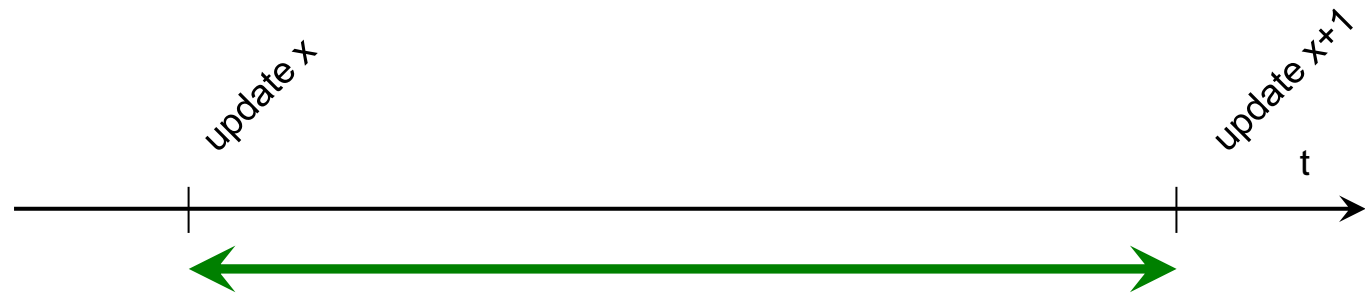
 Mi szükséges a YARA használatához?

 Mennyire hatékony a YARA?

# Védelmek frissítései

1990

Frissítések  
havonta/negyedévente

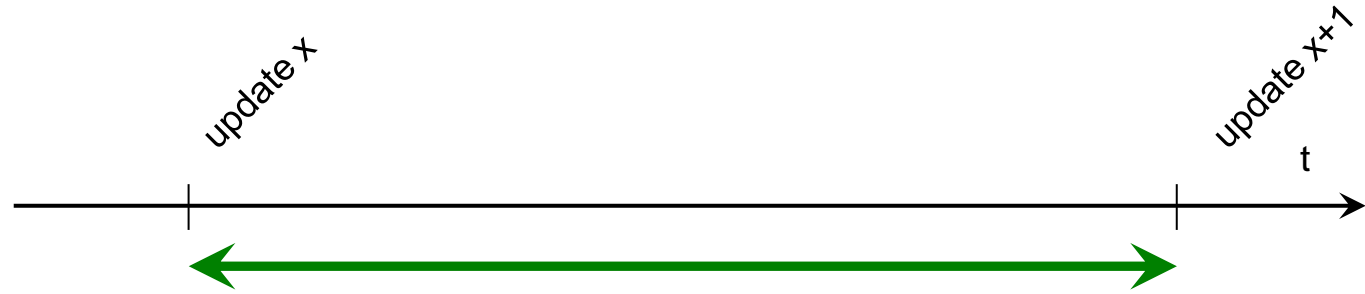


105  
vírus  
listája

# Védelmek frissítései

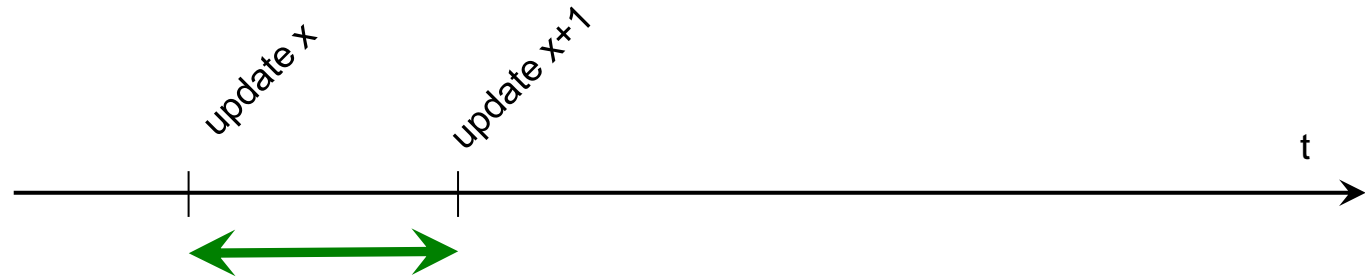
**1990**

Frissítések  
havonta/negyedévente



**2000**

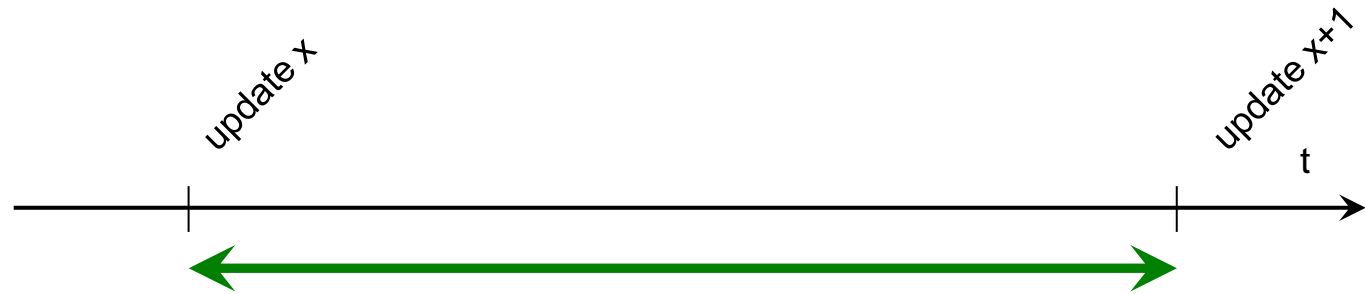
Frissítések  
naponta



# Védelmek frissítései

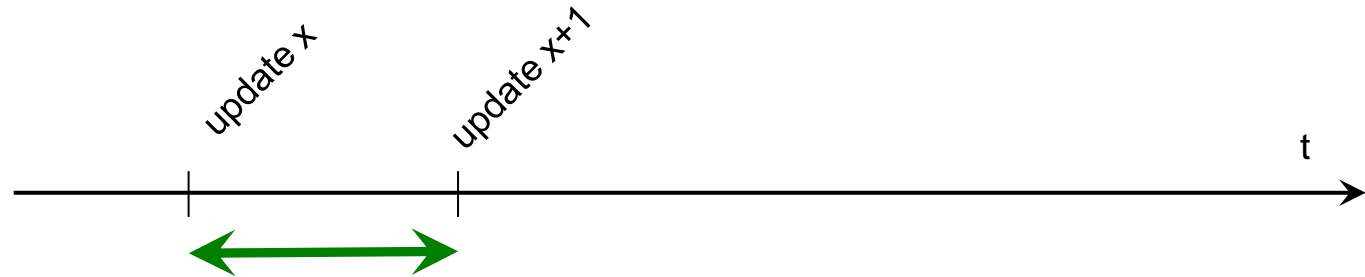
**1990**

Frissítések  
havonta/negyedévente



**2000**

Frissítések  
naponta



**2010**

Felhő használata



# Felhő alapú biztonság



Trend Micro  
Smart Protection Network  
Tuesday, 14 Sep. 2010

E-mail ellenőrzések  
**6.2 milliárd**

E-mail blokkolások  
**4.4 milliárd**

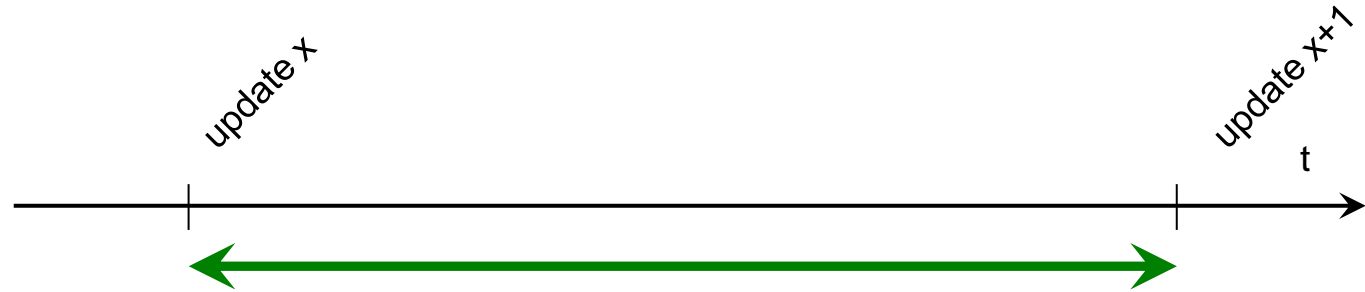
Webcím ellenőrzések  
**41 milliárd**

Webcím blokkolások  
**585 millió**

# Védelmek frissítései

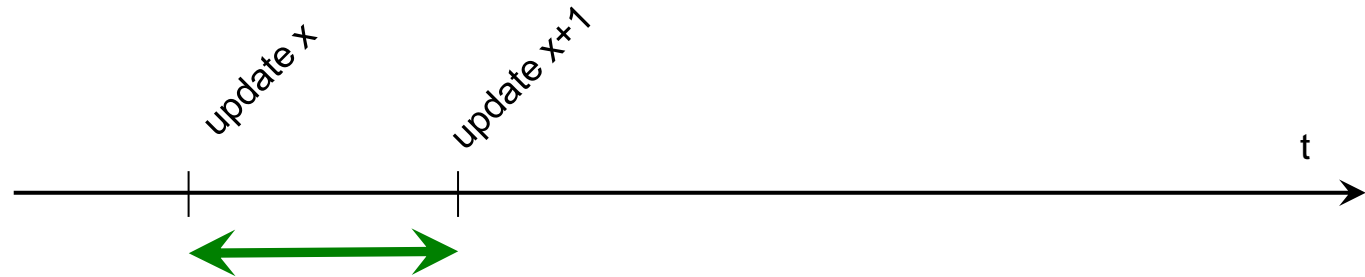
**1990**

Frissítések  
havonta/negyedévente



**2000**

Frissítések  
naponta



**2010**

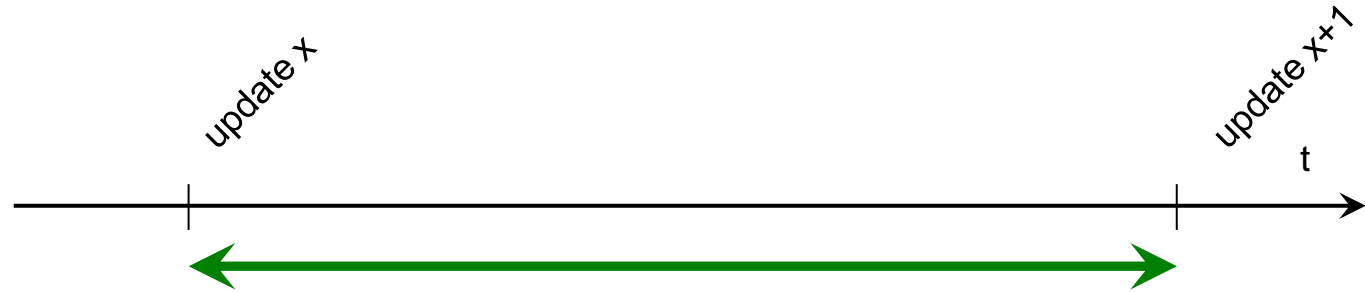
Felhő használata



# Védelmek frissítései

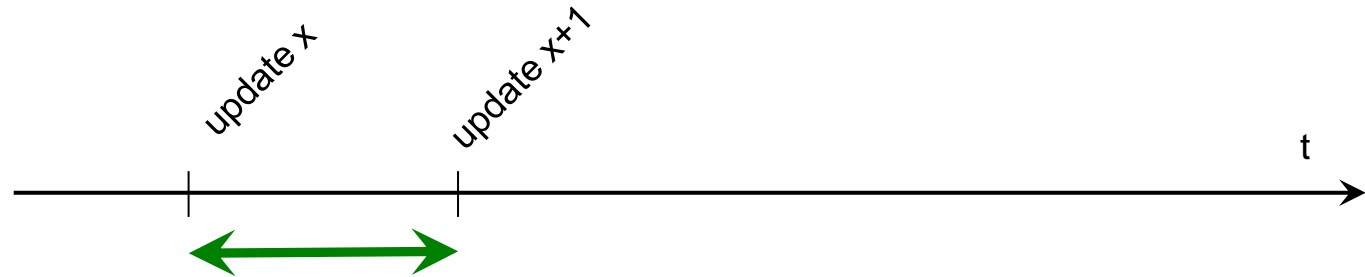
**1990**

Frissítések  
havonta/negyedévente



**2000**

Frissítések  
naponta



**2010**

Felhő használata

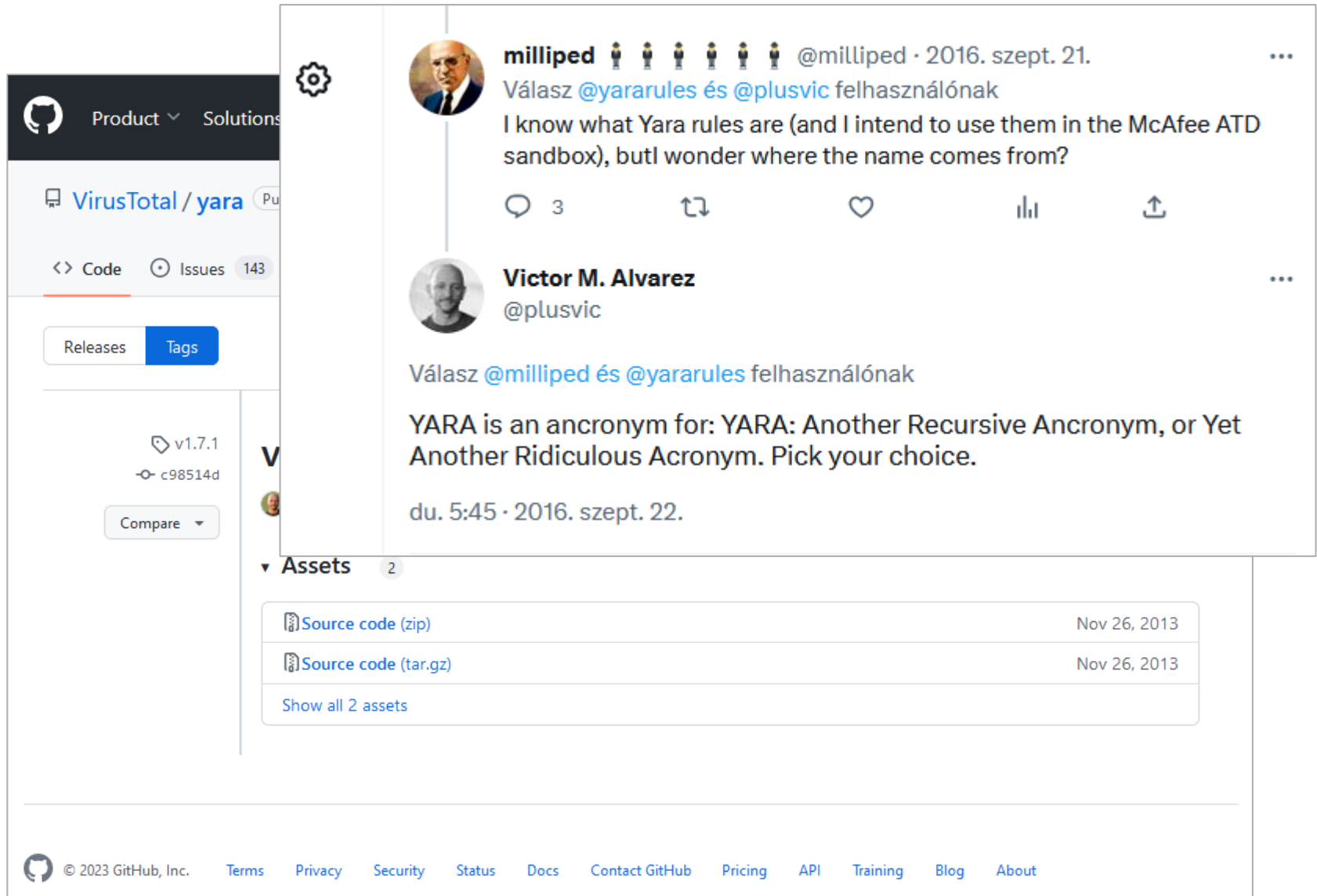


**2020**

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



# A YARA eredete



The image shows a GitHub repository page for VirusTotal / yara on the left and a Twitter thread on the right. The GitHub page includes navigation for Code, Issues, and Tags, with the Tags tab selected. It shows version v1.7.1 and a list of assets including source code in zip and tar.gz formats. The Twitter thread features a tweet from @milliped asking about the origin of the name YARA, and a reply from @plusvic explaining that YARA is an acronym for 'YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym'.

**GitHub Repository: VirusTotal / yara**

- Code Issues 143
- Releases Tags
- v1.7.1 c98514d
- Compare
- Assets (2)
  - Source code (zip) Nov 26, 2013
  - Source code (tar.gz) Nov 26, 2013
  - Show all 2 assets

**Twitter Thread:**

**milliped** @milliped · 2016. szept. 21.  
Válasz @yararules és @plusvic felhasználónak  
I know what Yara rules are (and I intend to use them in the McAfee ATD sandbox), but I wonder where the name comes from?

**Victor M. Alvarez** @plusvic  
Válasz @milliped és @yararules felhasználónak  
YARA is an acronym for: YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym. Pick your choice.  
du. 5:45 · 2016. szept. 22.

# YARA szabály

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

# YARA szabály

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

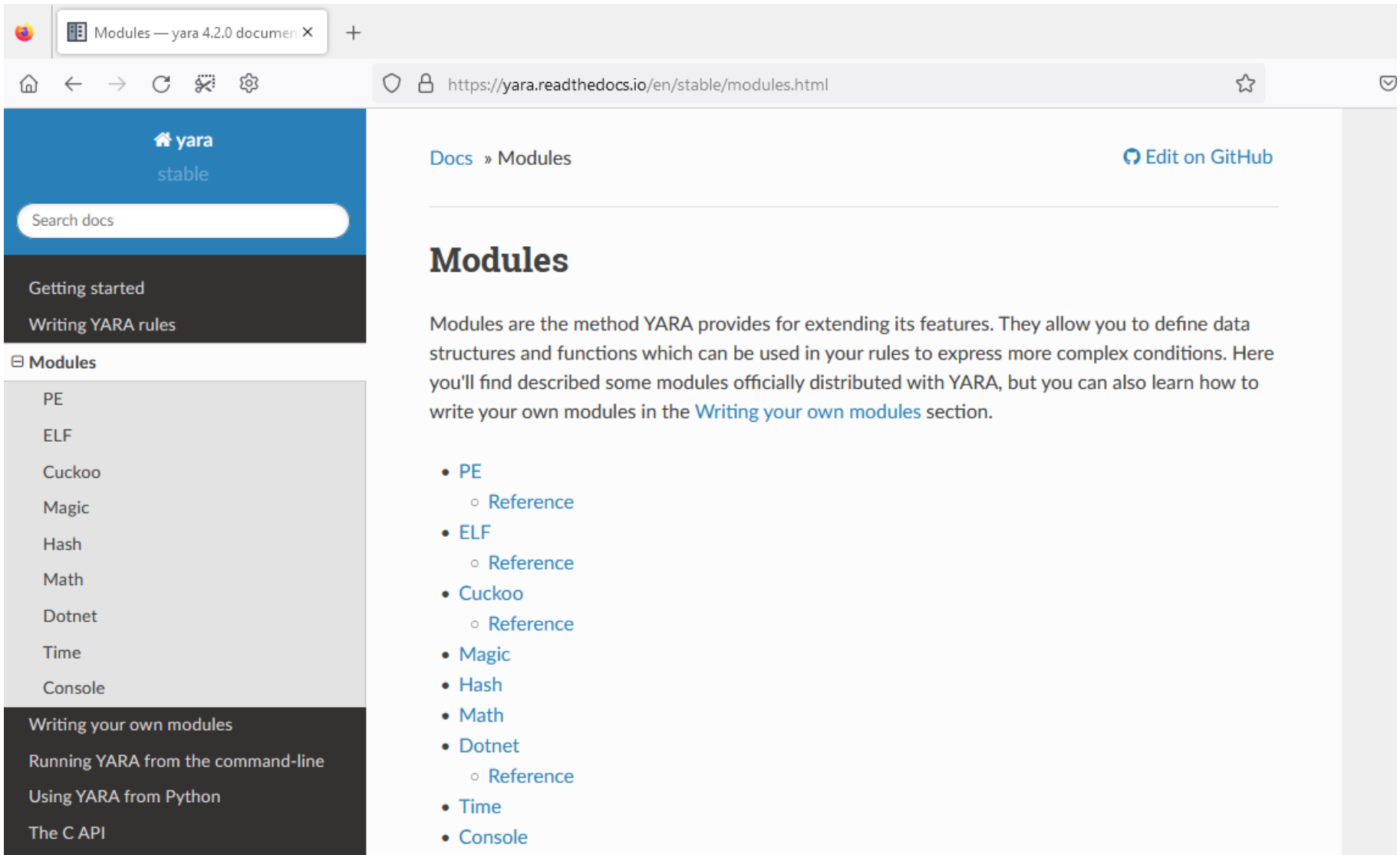
# YARA szabály

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

# YARA szabály

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

# YARA modulok



The screenshot shows a web browser displaying the YARA documentation page for 'Modules'. The browser's address bar shows the URL <https://yara.readthedocs.io/en/stable/modules.html>. The page features a blue header with the 'yara stable' logo and a search bar. A left sidebar contains a navigation menu with items like 'Getting started', 'Writing YARA rules', and 'Modules'. The main content area has a breadcrumb 'Docs » Modules', an 'Edit on GitHub' link, and a large heading 'Modules'. Below the heading is a paragraph explaining that modules are used to extend YARA's features and lists several modules with links to their respective reference pages.

Modules — yara 4.2.0 document X

https://yara.readthedocs.io/en/stable/modules.html




Docs » Modules [Edit on GitHub](#)

## Modules

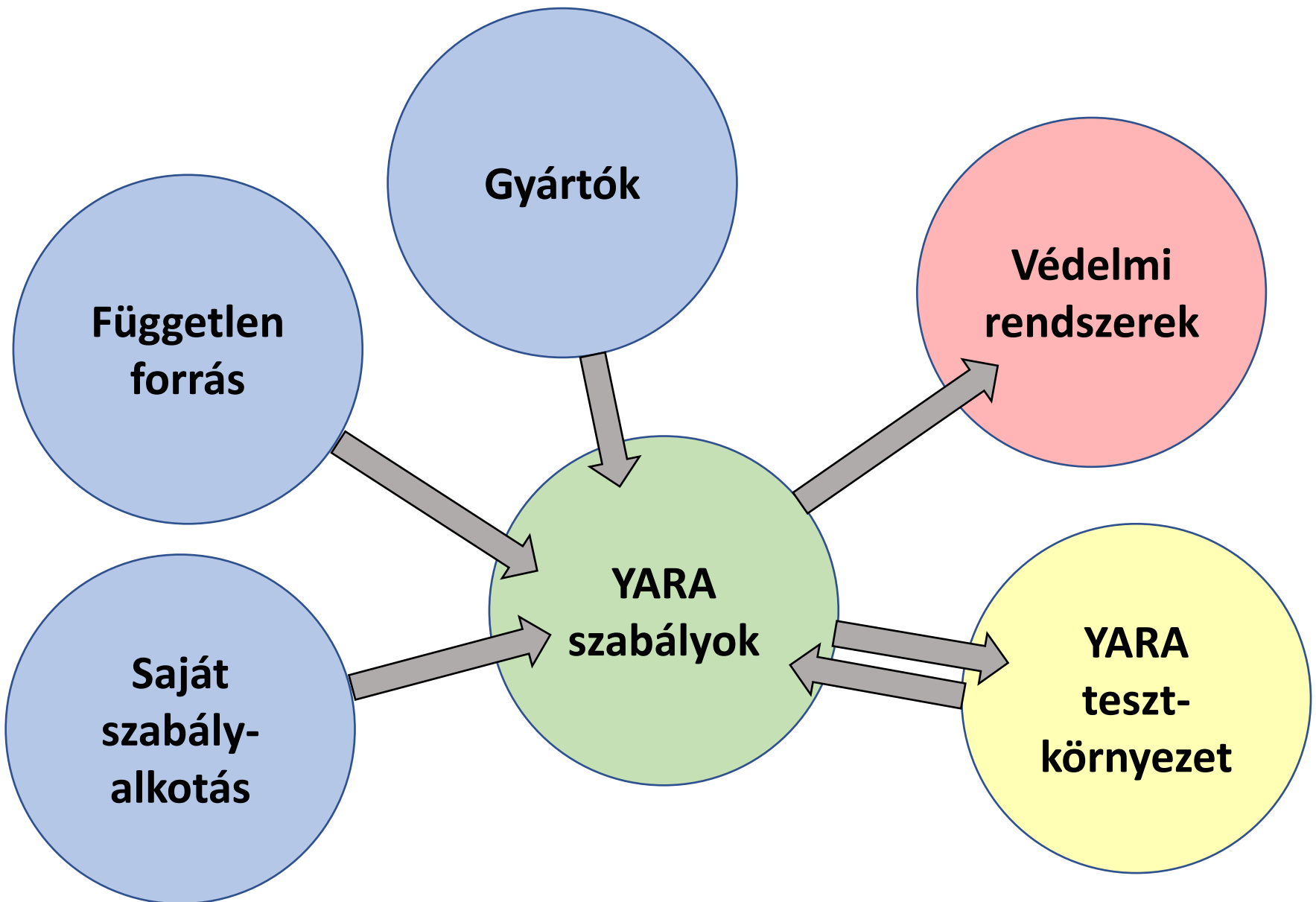
Modules are the method YARA provides for extending its features. They allow you to define data structures and functions which can be used in your rules to express more complex conditions. Here you'll find described some modules officially distributed with YARA, but you can also learn how to write your own modules in the [Writing your own modules](#) section.

- [PE](#)
  - [Reference](#)
- [ELF](#)
  - [Reference](#)
- [Cuckoo](#)
  - [Reference](#)
- [Magic](#)
- [Hash](#)
- [Math](#)
- [Dotnet](#)
  - [Reference](#)
- [Time](#)
- [Console](#)

# A YARA előnyei

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

# YARA használata





# Mennyire hatékony a YARA?

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

EDF TOOL S

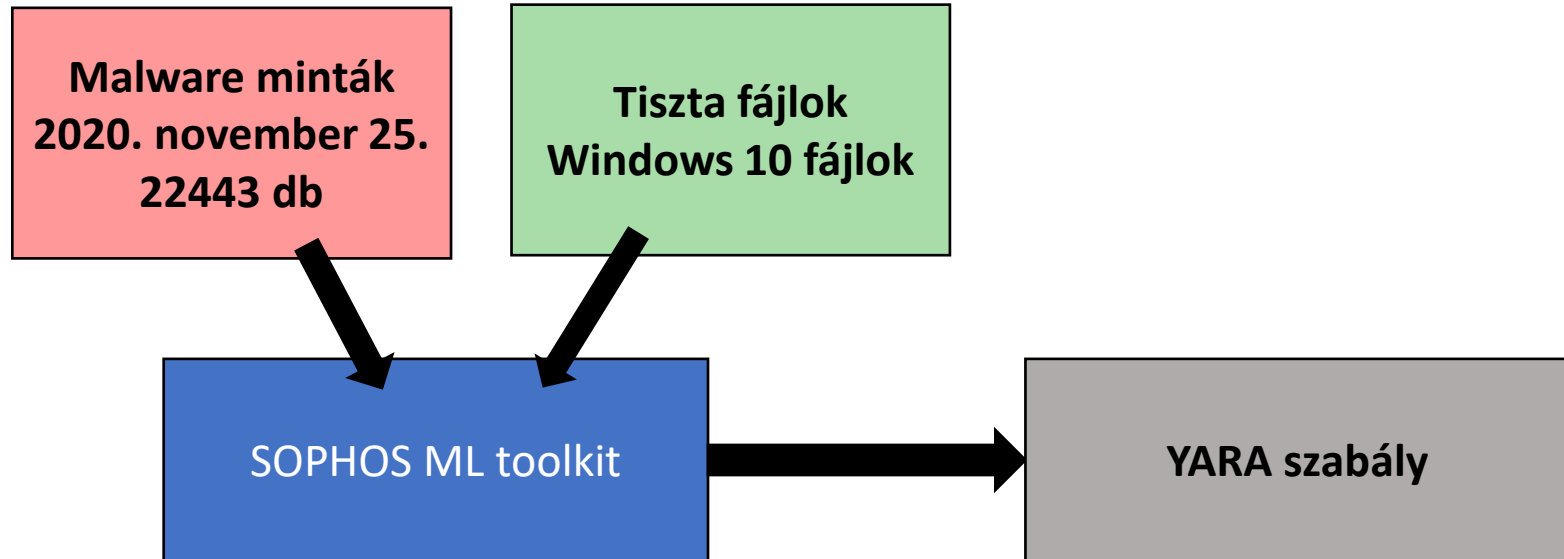
INCIDENT RESPONSE TOOL S

OPEN SOURCE

SECURITY OPERATIONS

THREAT HUNTING TOOL S

# Mennyire hatékony a YARA?

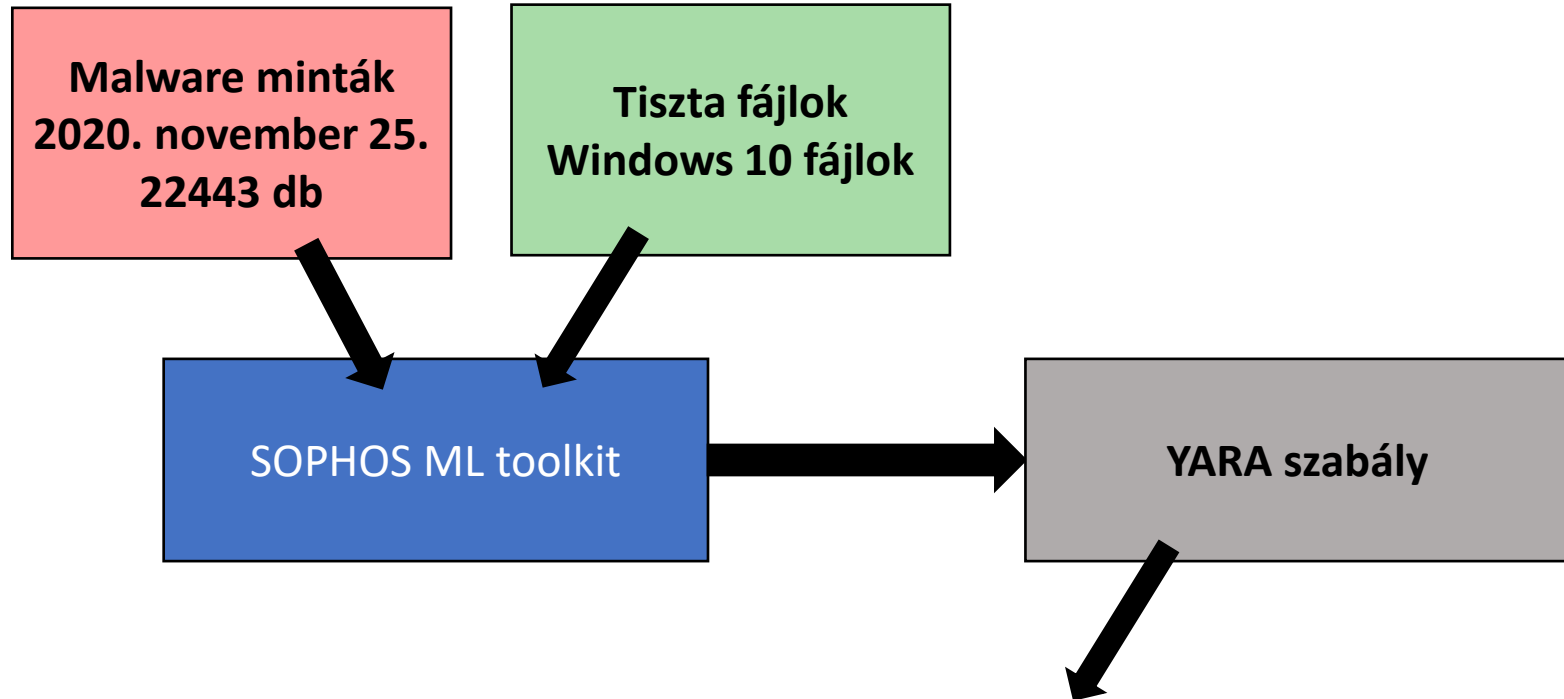


# Mennyire hatékony a YARA?

```
/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 = "rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr9999" fullword // weight: 2.227
    $s8 = "vbaExceptionHandler" fullword // weight: 2.198
    $s9 = "WNetEnumResourceA" fullword // weight: 2.129
    $s10 = "giiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiJkMkKkkkkkkknnn" 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 = "InitializeListHead" 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 = "qRqRqRqRepRePpRRichqR" 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) + (#s8 * 2.198) + (#s9 * 2.129) + (#s10 * 1.966) + (#s11 * 1.928) + (#s12 * 1.908) + (#s13 * 1.858) + (#s14 * 1.747) + (#s15 * 1.628) + (#s16 * 1.413) + (#s17 * 1.392) + (#s18 * 1.29) + (#s19 * 1.221) + (#s20 * 1.143) + (#s21 * 1.133) + (#s22 * 0.937) + (#s23 * 0.905) + (#s24 * 0.882) + (#s25 * 0.764) + (#s26 * 0.749) + (#s27 * 0.648) + (#s28 * 0.569) + (#s29 * 0.562) + (#s30 * 0.560) + (#s31 * 0.560) + (#s32 * 0.560) + (#s33 * 0.530) + (#s34 * 0.529) + (#s35 * 0.529) + (#s36 * 0.528) + (#s37 * 0.522) + (#s38 * 0.504) + (#s39 * 0.491) + (#s40 * 0.487) + (#s41 * 0.487) + (#s42 * 0.487) + (#s43 * 0.483) + (#s44 * 0.459) + (#s45 * 0.408) + (#s46 * 0.380) + (#s47 * 0.378) + (#s48 * 0.365) + (#s49 * 0.295) + (#s50 * 0.283) + (#s51 * 0.256) + (#s52 * 0.242) + (#s53 * 0.228) + (#s54 * 0.225) + (#s55 * 0.218) + (#s56 * 0.217) + (#s57 * 0.204) + (#s58 * 0.193) + (#s59 * 0.187) + (#s60 * 0.164) + (#s61 * 0.161) + (#s62 * 0.153) + (#s63 * 0.152) + (#s64 * 0.148) + (#s65 * 0.127) + (#s66 * 0.117) + (#s67 * 0.117) + (#s68 * 0.117) + (#s69 * 0.114) + (#s70 * 0.113) + (#s71 * 0.113) + (#s72 * 0.111) + (#s73 * 0.111) + (#s74 * 0.094) + (#s75 * 0.090) + (#s76 * 0.076) + (#s77 * 0.073) + (#s78 * 0.073) + (#s79 * 0.070) + (#s80 * 0.070) + (#s81 * 0.070) + (#s82 * 0.067) + (#s83 * 0.067) + (#s84 * 0.067) + (#s85 * 0.067) + (#s86 * 0.065) + (#s87 * 0.051) + (#s88 * 0.048) + (#s89 * 0.044) + (#s90 * 0.034) + (#s91 * 0.029) + (#s92 * 0.029) + (#s93 * 0.027) + (#s94 * 0.027) + (#s95 * 0.023) + (#s96 * 0.022) + (#s97 * 0.020) + (#s98 * 0.015) + (#s99 * 0.014) + (#s100 * 0.008) + (#s101 * 0.007) + (#s102 * 0.007) + (#s103 * 0.007) + (#s104 * 0.007) + (#s105 * 0.007) + (#s106 * 0.002) + (#s107 * -0.002) + (#s108 * -0.003) + (#s109 * -0.009) + (#s110 * -0.009) + (#s111 * -0.009) + (#s112 * -0.014) + (#s113 * -0.014) + (#s114 * -0.017) + (#s115 * -0.018) + (#s116 * -0.021) + (#s117 * -0.024) + (#s118 * -0.024) + (#s119 * -0.038) + (#s120 * -0.039) + (#s121 * -0.039) + (#s122 * -0.039) + (#s123 * -0.040) + (#s124 * -0.040) + (#s125 * -0.046) + (#s126 * -0.056) + (#s127 * -0.098) + (#s128 * -0.104) + (#s129 * -0.104) + (#s130 * -0.109) + (#s131 * -0.109) + (#s132 * -0.134) + (#s133 * -0.138) + (#s134 * -0.158) + (#s135 * -0.160) + (#s136 * -0.160) + (#s137 * -0.179) + (#s138 * -0.190) + (#s139 * -0.190) + (#s140 * -0.190) + (#s141 * -0.191) + (#s142 * -0.196) + (#s143 * -0.198) + (#s144 * -0.204) + (#s145 * -0.208) + (#s146 * -0.212) + (#s147 * -0.222) + (#s148 * -0.239) + (#s149 * -0.239) + (#s150 * -0.241) + (#s151 * -0.242) + (#s152 * -0.258) + (#s153 * -0.263) + (#s154 * -0.288) + (#s155 * -0.324) + (#s156 * -0.331) + (#s157 * -0.332) + (#s158 * -0.332) + (#s159 * -0.339) + (#s160 * -0.341) + (#s161 * -0.341) + (#s162 * -0.342) + (#s163 * -0.351) + (#s164 * -0.351) + (#s165 * -0.386) + (#s166 * -0.386) + (#s167 * -0.386) + (#s168 * -0.402) + (#s169 * -0.411) + (#s170 * -0.411) + (#s171 * -0.427) + (#s172 * -0.430) + (#s173 * -0.430) + (#s174 * -0.430) + (#s175 * -0.430) + (#s176 * -0.430) + (#s177 * -0.430) + (#s178 * -0.430) + (#s179 * -0.430) + (#s180 * -0.430) + (#s181 * -0.430) + (#s182 * -0.430) + (#s183 * -0.430) + (#s184 * -0.430) + (#s185 * -0.430) + (#s186 * -0.430) + (#s187 * -0.430) + (#s188 * -0.430) + (#s189 * -0.430) + (#s190 * -0.430) + (#s191 * -0.430) + (#s192 * -0.430) + (#s193 * -0.430) + (#s194 * -0.430) + (#s195 * -0.430) + (#s196 * -0.430) + (#s197 * -0.430) + (#s198 * -0.430) + (#s199 * -0.430) + (#s200 * -0.430) + (#s201 * -0.430) + (#s202 * -0.430) + (#s203 * -0.430) + (#s204 * -0.430) + (#s205 * -0.430) + (#s206 * -0.430) + (#s207 * -0.430) + (#s208 * -0.430) + (#s209 * -0.430) + (#s210 * -0.430) + (#s211 * -0.430) + (#s212 * -0.430) + (#s213 * -0.430) + (#s214 * -0.430) + (#s215 * -0.430) + (#s216 * -0.430) + (#s217 * -0.430) + (#s218 * -0.430) + (#s219 * -0.430) + (#s220 * -0.430) + (#s221 * -0.430) + (#s222 * -0.430) + (#s223 * -0.430) + (#s224 * -0.430) + (#s225 * -0.430) + (#s226 * -0.430) + (#s227 * -0.430) + (#s228 * -0.430) + (#s229 * -0.430) + (#s230 * -0.430) + (#s231 * -0.430) + (#s232 * -0.430) + (#s233 * -0.430) + (#s234 * -0.430) + (#s235 * -0.430) + (#s236 * -2.914) + (#s237 * -3.421) + (#s238 * -3.52) + (#s239 * -6.123) + (#s240 * -7.009)
```

# Mennyire hatékony a YARA?



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

**91,45% - 96,25%**

Windows fájlok:

**0,33%**

További részletek: [www.yaralab.eu](http://www.yaralab.eu)

