YARA调研报告

简介

YARA 是一个帮助恶意软件研究人员识别和分类恶意软件样本的工具，由VirusTotal开源（GPL协议），基于静态分析识别恶意软件样本

目前使用 YARA 的知名软件有赛门铁克、火眼、卡巴斯基、McAfee等。

源码：https://github.com/VirusTotal/yara

文档：https://yara.readthedocs.org/

使用方法

本地安装和使用

1. 下载安装包https://github.com/VirusTotal/yara/releases.
2. 安装依赖库

```
sudo apt-get install automake libtool make gcc pkg-config
```

3. 解压并安装

```
tar -zxf yara-4.1.0.tar.gz
cd yara-4.1.0
./bootstrap.sh
./configure
make
sudo make install
```

4. 检查是否安装成功

```
make check
```

Docker用法

Docker:https://github.com/blacktop/docker-yara

```
docker pull blacktop/yara
```

使用

提前将yara规则下载并放置在指定目录

```
alias yara='docker run -it --rm -v $(pwd):/malware:ro blacktop/yara $@' yara -w -g [规则.yar] [文件目录]
```

这种方法每次启动容器都会先对规则进行编译(对500个规则编译花费了5秒钟)

输出结果后退出并删除容器，若再次使用yara命令会重新对规则编译

输出样例如下，下载的恶意样本来自于https://www.stratosphereips.org/datasets-malware

> suspicious_packer_section [packer,PE]
> ./work/malware/39UvZmv.exe IsPE32 [PECheck] ./work/malware/39UvZmv.exe IsWindowsGUI [PECheck] ./work/malware/39UvZmv.exe IsPacked [PECheck] ./work/malware/39UvZmv.exe HasOverlay [PECheck] ./work/malware/39UvZmv.exe SEH_Init [Tactic_DefensiveEvasion,Technique_AntiDebugging,SubTechnique_SEH]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe anti_dbg []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe win_registry []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe win_files_operation []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Str_Win32_Winsock2_Library []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Str_Win32_Wininet_Library []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Str_Win32_Internet_API []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe CRC32_poly_Constant []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe CRC32_table []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe RijnDael_AES []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe RijnDael_AES_CHAR []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe maldoc_indirect_function_call_3 [maldoc]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe maldoc_getEIP_method_1 [maldoc]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe MS17_010_WanaCry_worm []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe WannaDecryptor [WannaDecryptor]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe NHS_Strain_Wanna [NHS_Strain_Wanna]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Wanna_Cry_Ransomware_Generic []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe WannaCry_Ransomware []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe WannaCry_Ransomware_Gen []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe WannaCry_Ransomware_Dropper []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe WannaCry_SMB_Exploit []
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe wannacry_static_ransom [wannacry_static_ransom] ./work/malware/05a00c320754934782ec5dec1d5c0476.exe worm_ms17_010 [worm_ms17_010] ./work/malware/05a00c320754934782ec5dec1d5c0476.exe IsPE32 [PECheck] ./work/malware/05a00c320754934782ec5dec1d5c0476.exe IsWindowsGUI [PECheck] ./work/malware/05a00c320754934782ec5dec1d5c0476.exe IsPacked [PECheck]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe HasRichSignature [PECheck]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Microsoft_Visual_Cpp_v60 [PEiD]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe

> Microsoft_Visual_Cpp_v50v60_MFC_additional [PEiD]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Microsoft_Visual_Cpp_50 [PEiD]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Microsoft_Visual_Cpp_v50v60_MFC [PEiD]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe Microsoft_Visual_Cpp [PEiD]
> ./work/malware/05a00c320754934782ec5dec1d5c0476.exe

Python用法

参考于：https://yara.readthedocs.io/en/stable/yarapython.html

依赖于`yara-python`库，进行检测

```
import yara

# 基于指定的目录编译规则
rules = yara.compile(filepath='./rules')

# 或者直接基于字符串编译
rules_single = yara.compile(source='rule dummy { condition: true }')

# 将文件与规则匹配
matches = rules.match('/foo/bar/my_file')

# 将文件与进程匹配
matches_pid = rules.match(pid=1234)

```

因为每次规则的编译会耗费时间，所以可以将编译好的规则保存为一个二进制文件

```
# 将编译后的规则进行保存
rules.save('/foo/bar/my_compiled_rules')

# 导入已经编译过的规则
rules = yara.load('/foo/bar/my_compiled_rules')
```

注意事项

①恶意文件压缩后破坏了原有的二进制序列，yara并不能智能解压并检测，需要先识别压缩包文件，递归解压后再检测

规则编写

规则编写可以参考于https://yara.readthedocs.io/en/stable/writingrules.html

例如下述规则是基于16进制字符串进行匹配，？可以匹配任何内容

```
rule WildcardExample
{
    strings:
        $hex_string = { E2 34 ?? C8 A? FB }

    condition:
        $hex_string
}
```

规则集

① Yara-Rules

地址：https://github.com/Yara-Rules/rules，目前已有2.7K Star

简介

该项目在2015年成立，用于汇聚各种不同的yara规则，遵循GNU-GPLv2开放许可

规则

项目中总共包含13个文件夹，12类规则，具体情况如下

名称	描述
Anti-debug/Anti-VM	用于检测文件中存在的反调试和反虚拟化技术
CVE Rules	用于检测对通用漏洞（CVE,Common Vulnerabilities and Exposures）的利用（包含了14个CVE漏洞）
Crypto	检测文件中存在的密码学算法
Exploit Kits	用于检测Exploit集合工具（用于进行传播，程序漏洞的利用和管理控制台等）
Malicious Documents	检测是否有利用恶意代码的文档
malware	检测知名恶意软件*
Packers	检测恶意软件用来隐藏自身的知名软件包
webshells	用来识别知名的webshells
email	检测恶意邮件
Malware Mobile	检测移动端的恶意软件
Capabilities	不属于以上类别的其他规则
Deprecated	已经被废弃的规则

其中malware目录下包含了361个yar文件，具体如下

```
000_common_rules.yar         APT_WildNeutron.yar     MALW_MacControl.yar
POS_Mozart.yar APT_APT10.yar           APT_Windigo_Onimiki.yar   MALW_Madness.yar
POS.yar APT_APT15.yar          APT_Winnti.yar      MALW_Magento_backend.yar
RANSOM_777.yar APT_APT17.yar           APT_WoolenGoldfish.yar
MALW_Magento_frontend.yar      RANSOM_acroware.yar APT_APT1.yar
EXPERIMENTAL_Beef.yar     MALW_Magento_suspicious.yar      RANSOM_Alpha.yar
APT_APT29_Grizzly_Steppe.yar      GEN_PowerShell.yar    MALW_Mailers.yar
RANSOM_BadRabbit.yar APT_APT3102.yar           MalConfScan.yar     MALW_marap.yar
RANSOM_Cerber.yar APT_APT9002.yar          MALW_adwind_RAT.yar
MALW_MedusaHTTP_2019.yar     RANSOM_Comodosec.yar APT_Backspace.yar
MALW_AgentTesla_SMTP.yar  MALW_Miancha.yar       RANSOM_Crypren.yar APT_Bestia.yar
MALW_AgentTesla.yar     MALW_MiniAsp3_mem.yar        RANSOM_Cryptolocker.yar
APT_Blackenergy.yar        MALW_Alina.yar      MALW_Mirai_Okiru_ELF.yar
RANSOM_CryptoNar.yar APT_Bluetermite_Emdivi.yar      MALW_AlMashreq.yar
MALW_Mirai_Satori_ELF.yar      RANSOM_.CRYPTXXX.yar APT_C16.yar
MALW_Andromeda.yar    MALW_Mirai.yar         RANSOM_DMALocker.yar APT_Carbanak.yar
MALW_Arkei.yar      MALW_Miscelanea_Linux.yar      RANSOM_DoublePulsar_Petya.yar
APT_Careto.yar           MALW_Athena.yar     MALW_Miscelanea.yar
RANSOM_Erebus.yar APT_Casper.yar           MALW_ATM_HelloWorld.yar
MALW_Monero_Miner_installer.yar    RANSOM_GoldenEye.yar APT_CheshireCat.yar
MALW_Atmos.yar      MALW_MSILStealer.yar       RANSOM_GPGQwerty.yar
APT_Cloudduke.yar         MALW_ATMPot.yar     MALW_Naikon.yar
RANSOM_jeff_dev.yar APT_Cobalt.yar           MALW_AZORULT.yar
MALW_Naspyupdate.yar       RANSOM_locdoor.yar APT_Codoso.yar
MALW_BackdoorSSH.yar    MALW_NetTraveler.yar       RANSOM_Locky.yar
APT_CrashOverride.yar         MALW_Backoff.yar    MALW_NionSpy.yar
RANSOM_Maze.yar APT_DeepPanda_Anthem.yar       MALW_Bangat.yar     MALW_Notepad.yar
RANSOM_MS17-010_Wannacrypt.yar APT_DeputyDog.yar         MALW_Batel.yar
MALW_NSFree.yar        RANSOM_PetrWrap.yar APT_Derusbi.yar
MALW_BlackRev.yar     MALW_Odinaff.yar       RANSOM_Petya_MS17_010.yar
APT_DPRK_ROKRAT.yar        MALW_BlackWorm.yar    MALW_Olyx.yar
RANSOM_Petya.yar APT_Dubnium.yar           MALW_Boouset.yar    MALW_OSX_Leverage.yar
RANSOM_Pico.yar APT_Duqu2.yar          MALW_Bublik.yar     MALW_PE_sections.yar
RANSOM_SamSam.yar APT_Emissary.yar         MALW_Buzus_Softpulse.yar
MALW_PittyTiger.yar        RANSOM_Satana.yar APT_EnergeticBear_backdoored_ssh.yar
MALW_CAP_HookExKeylogger.yar  MALW_PolishBankRat.yar
RANSOM_screenlocker_5h311_1nj3c706.yar APT_eqgrp_apr17.yar         MALW_Chicken.yar
MALW_Ponmocup.yar        RANSOM_Shiva.yar APT_EQUATIONGRP.yar
MALW_Citadel.yar    MALW_Pony.yar          RANSOM_shrug2.yar APT_Equation.yar
MALW_Cloaking.yar     MALW_Predator.yar        RANSOM_Sigma.yar
APT_fancybear_dnc.yar         MALW_Cookies.yar    MALW_PubSab.yar
RANSOM_Snake.yar APT_fancybear_downdelph.yar       MALW_Corkow.yar
MALW_PurpleWave.yar        RANSOM_Stampado.yar APT_FiveEyes.yar
MALW_Cxpid.yar      MALW_Pyinstaller.yar       RANSOM_termite.yar APT_furtim.yar
MALW_Cythosia.yar     MALW_PyPI.yar          RANSOM_TeslaCrypt.yar
APT_FVEY_ShadowBrokers_Jan17_Screen_Strings.yar  MALW_DDoSTf.yar
MALW_Quarian.yar       RANSOM_Tox.yar APT_Grasshopper.yar         MALW_Derkziel.yar
```

```
MALW_Rebirth_Vulcan_ELF.yar      RAT_Adwind.yar APT_Greenbug.yar
MALW_Dexter.yar     MALW_Regsubdat.yar       RAT_Adzok.yar
APT_Grizzlybear_uscert.yar       MALW_DiamondFox.yar     MALW_Retefe.yar
RAT_Asyncrat.yar APT_HackingTeam.yar         MALW_DirtJumper.yar
MALW_Rockloader.yar        RAT_BlackShades.yar APT_Hellsing.yar
MALW_Eicar.yar      MALW_Rooter.yar        RAT_Bolonyokte.yar APT_HiddenCobra.yar
MALW_Elex.yar       MALW_Rovnix.yar        RAT_Bozok.yar APT_Hikit.yar
MALW_Elknot.yar     MALW_Safenet.yar       RAT_Cerberus.yar APT_Industroyer.yar
MALW_Emotet.yar     MALW_Sakurel.yar       RAT_Crimson.yar APT_Irontiger.yar
MALW_Empire.yar     MALW_Sayad.yar         RAT_CrossRAT.yar APT_Kaba.yar
MALW_Enfal.yar      MALW_Scarhikn.yar        RAT_CyberGate.yar
APT_Ke3Chang_TidePool.yar      MALW_Exploit_UAC_Elevators.yar  MALW_Sendsafe.yar
RAT_DarkComet.yar APT_KeyBoy.yar           MALW_Ezcob.yar      MALW_Shamoon.yar
RAT_FlyingKitten.yar APT_LotusBlossom.yar        MALW_F0xy.yar
MALW_shifu_shiz.yar        RAT_Gh0st.yar APT_Minidionis.yar         MALW_FakeM.yar
MALW_Shifu.yar         RAT_Gholee.yar APT_Mirage.yar          MALW_FALLCHILL.yar
MALW_sitrof_fortis_scar.yar      RAT_Glass.yar APT_Molerats.yar
MALW_Fareit.yar     MALW_Skeleton.yar        RAT_Havex.yar APT_Mongall.yar
MALW_Favorite.yar     MALW_Spora.yar         RAT_Hizor.yar APT_MoonlightMaze.yar
MALW_FUDCrypt.yar     MALW_Sqlite.yar        RAT_Indetectables.yar APT_NGO.yar
MALW_Furtim.yar     MALW_Stealer.yar       RAT_Inocnation.yar APT_Oilrig.yar
MALW_Gafgyt.yar     MALW_Surtr.yar         RAT_jRAT.yar APT_OpClandestineWolf.yar
MALW_Genome.yar     MALW_T5000.yar         RAT_Meterpreter_Reverse_Tcp.yar
APT_OPCleaver.yar        MALW_Glasses.yar    MALW_Tedroo.yar        RAT_Nanocore.yar
APT_OpDustStorm.yar          MALW_Gozi.yar       MALW_Tinba.yar
RAT_NetwiredRC.yar APT_OpPotao.yar           MALW_Grozlex.yar
MALW_TinyShell_Backdoor_gen.yar    RAT_Njrat.yar APT_Passcv.yar
MALW_Hajime.yar     MALW_Torte_ELF.yar       RAT_Orcus.yar APT_PCclient.yar
MALW_hancitor.yar     MALW_TreasureHunt.yar        RAT_PlugX.yar APT_Pipcreat.yar
MALW_Hsdfihdf_banking.yar   MALW_TrickBot.yar        RAT_PoetRATDoc.yar
APT_Platinum.yar        MALW_Httpsd_ELF.yar     MALW_TRITON_HATMAN.yar
RAT_PoetRATPython.yar APT_Poseidon_Group.yar         MALW_IcedID.yar
MALW_TRITON_ICS_FRAMEWORK.yar      RAT_PoisonIvy.yar APT_Prikormka.yar
MALW_Iexpl0ree.yar    MALW_Trumpbot.yar        RAT_Ratdecoders.yar
APT_PutterPanda.yar        MALW_IMuler.yar     MALW_Upatre.yar        RAT_Sakula.yar
APT_RedLeaves.yar         MALW_Install11.yar    MALW_Urausy.yar
RAT_ShadowTech.yar APT_Regin.yar           MALW_Intel_Virtualization.yar
MALW_Vidgrab.yar       RAT_Shim.yar APT_RemSec.yar          MALW_IotReaper.yar
MALW_viotto_keylogger.yar      RAT_Terminator.yar APT_Sauron_extras.yar
MALW_Jolob_Backdoor.yar   MALW_Virut_FileInfector_UNK_VERSION.yar  RAT_xRAT20.yar
APT_Sauron.yar          MALW_Kelihos.yar    MALW_Volgmer.yar       RAT_xRAT.yar
APT_Scarab_Scieron.yar        MALW_KeyBase.yar    MALW_Wabot.yar
RAT_Xtreme.yar APT_Seaduke.yar           MALW_KINS.yar       MALW_Warp.yar
RAT_ZoxPNG.yar APT_Shamoon_StoneDrill.yar      MALW_kirbi_mimikatz.yar
MALW_Wimmie.yar        TOOLKIT_Chinese_Hacktools.yar APT_Snowglobe_Babar.yar
MALW_Korlia.yar     MALW_xDedic_marketplace.yar      TOOLKIT_Dubrute.yar
APT_Sofacy_Bundestag.yar       MALW_Korplug.yar    MALW_XHide.yar
TOOLKIT_exe2hex_payload.yar APT_Sofacy_Fysbis.yar        MALW_Kovter.yar
MALW_XMRIG_Miner.yar       TOOLKIT_FinFisher_.yar APT_Sofacy_Jun16.yar
```

```
MALW_kpot.yar       MALW_XOR_DDos.yar        TOOLKIT_Gen_powerkatz.yar
APT_Sphinx_Moth.yar        MALW_Kraken.yar     MALW_Yayih.yar
TOOLKIT_Mandibule.yar APT_Stuxnet.yar          MALW_Kwampirs.yar
MALW_Yordanyan_ActiveAgent.yar     TOOLKIT_PassTheHash.yar APT_Terracota.yar
MALW_Lateral_Movement.yar   MALW_Zegost.yar        TOOLKIT_Powerstager.yar
APT_ThreatGroup3390.yar        MALW_Lenovo_Superfish.yar   MALW_Zeus.yar
TOOLKIT_Pwdump.yar APT_TradeSecret.yar         MALW_LinuxBew.yar
Operation_Blockbuster        TOOLKIT_Redteam_Tools_by_GUID.yar APT_Turla_Neuron.yar
MALW_LinuxHelios.yar    POS_Bernhard.yar       TOOLKIT_Redteam_Tools_by_Name.yar
APT_Turla_RUAG.yar         MALW_LinuxMoose.yar     POS_BruteforcingBot.yar
TOOLKIT_Solarwinds_credential_stealer.yar APT_Unit78020.yar        MALW_LostDoor.yar
POS_Easterjack.yar       TOOLKIT_THOR_HackTools.yar APT_UP007_SLServer.yar
MALW_LuaBot.yar     POS_FastPOS.yar        TOOLKIT_Wineggdrop.yar APT_Uppercut.yar
MALW_LuckyCat.yar     POS_LogPOS.yar APT_Waterbug.yar         MALW_LURK0.yar
POS_MalumPOS.yar
```

② awesome-yara

地址：https://github.com/InQuest/awesome-yara　目前已有1.6K Star

简介

一个收集各种yara规则、工具和资源的清单，主要是给出链接和简单描述

规则

收集了56个开源项目的yara规则，不同项目的yara规则来源于实验室收集或者个人收集，存在重复规则和无效规则

其中部分项目的规则已经很多年没有更新，有失效的可能性

工具

- 用于生成yara规则的工具
- 某些封装了yara的工具
- yara规则管理工具
- plyara : Pyhon用于解析yara的三方库