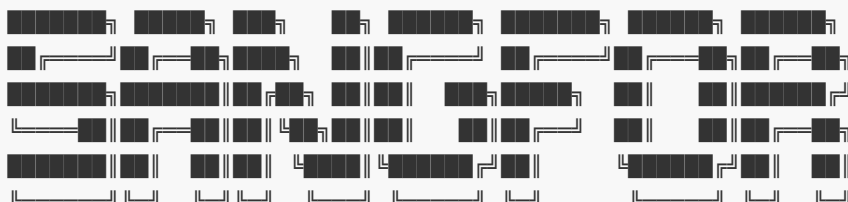


MMH(M78 Miner Helper)使用手册

Info

文件名: MMH1.3 (M78 Miner Helper)

版本: V1.3



```
#MMH--M78 Miner Helper . (C) 2021-2022 Sangfor_M78_In_ChangSha
Version:1.3
```

Usage: Example ./MMH1.3 -clean workminer

```
-list          列出当前支持检测查杀的病毒家族
-show         显示常见病毒的特征表述
-check [string] 检测主机是否存在指定类型的病毒
-CHECK        加载所有病毒模块扫描
-clean [string] 对指定的病毒类型一键查杀
-CLEAN        执行全部专杀模块
-PROC         检测当前系统进程中是否存在与历史病毒进程名相同的进程, 仅供参考
-rule yarafile yara扫描, 使用一下参数指定类型扫描
    -pid [int]    对系统进程pid进行yara扫描
    -PIDS         对系统全部进程进行yara扫描
    -d [dictory]  对目录进行yara扫描
    -f [string]   对文件进行yara扫描
-unhide       检测可能隐藏的系统进程, 仅作参考
-psfile       显示当前系统进程中的运行程序文件路径
-cron crontab 分析任务日志以快速定位可疑的计划任务
```

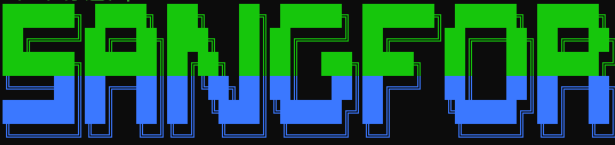
Example:

```
MMH1.3 -init 生成yara模板
MMH1.3 -rule /tmp/yara.yar -d /opt/ #yara扫描目录
MMH1.3 -rule /tmp/yara.yar -f /opt/virusfile #yara扫描文件
MMH1.3 -rule /tmp/yara.yar -pid pid #yara扫描单个进程
MMH1.3 -rule /tmp/yara.yar -PIDS #yara扫描全部进程
```

主要功能:

1. 查看使用说明, 在Linux中默认运行程序, 显示相关使用参数

```

root@MMH:~# ./MMH1.3
当前程序进程pid: 18501

#MMH--M78 Miner Helper . (C) 2021-2022 Sangfor_M78_In_ChangSha
Version:1.3
Usage: Example ./MMH -clean workminer
        -list          列出当前支持检测查杀的病毒家族
        -show          显示常见病毒的特征表述
        -check [string] 检测主机是否存在指定类型的病毒
        -CHECK         加载所有病毒模块扫描
        -clean [string] 对指定的病毒类型一键查杀
        -CLEAN         执行全部专杀模块
        -PROC          检测当前系统进程中是否存在与历史病毒进程名相同的进程，仅供参考
        -rule file     yara扫描，使用一下参数指定类型扫描
                        -pid [int]      对系统进程pid进行yara扫描
                        -PIDS           对系统全部进程进行yara扫描
                        -d [directory] 对目录进行yara扫描
                        -f [string]    对文件进行yara扫描
        -init          生成yara模板
        -unhide        检测可能隐藏的系统进程，仅作参考
        -psfile        显示当前系统进程中的运行程序文件路径
        -cron crontab  分析任务日志以快速定位可疑的计划任务

Example:
MMH1.3 -init 生成yara模板
MMH1.3 -rule /tmp/yara.yar -d /opt/ #yara扫描目录
MMH1.3 -rule /tmp/yara.yar -f /opt/virusfile #yara扫描文件
MMH1.3 -rule /tmp/yara.yar -pid pid #yara扫描单个进程
MMH1.3 -rule /tmp/yara.yar -PIDS #yara扫描全部进程
root@MMH:~# ./MMH1.3

```

2. 支持查杀的病毒家族

命令举例：./MMH1.3 -list 显示支持的病毒家族

```

MMHLog:2022/06/13 17:39:19.695348 当前支持的专杀有：
    autominer
    cleanfda
    fullskystar
    gates
    iptablesupdate
    javaupdateminer
    lh-miner
    moneroocean
    oznminer
    powerghost
    pwndns-1
    pwndns
    SHC-Miner
    SMBGghost
    systemdminer
    thegov
    vmwareminer
    warmup
    workminer
    xms8220
    xmssminer
    xorddos
root@MMH:~#

```

如果对这些病毒家族不了解，不知道命中的是不是这些家族，也可以通过 -show 参数查看这家病毒在系统中的常见特征

命令举例：./MMH1.3 -show

```

root@MMH:~# ./MMH1.3 -show
当前程序进程pid: 18568
autominer    挖矿家族,库文件劫持,文件/usr/local/lib/libc2.28.so,.git/kworkers,
              .git/dbus,.git/kworkers,.git/autoupdate
cleanfda     存在计划任务,免密登陆,/usr/bin/下面的curl,wget,top,ps,pstree被篡改,常见文件
              /etc/newinit.sh,/tmp/newinit.sh,/etc/zzh,/etc/zzh,/etc/etc
fullskystar  云矿挖矿,存在库文件劫持,通信fullskystar.top,常见文件/lib/libcurl.so.2.17.0,
              /usr/bin/bioset,/usr/bin/kthreadd
gates        gates木马在进程中会有一个/usr/bin/.sshd的进程,还有ps,netstat,lsof,ss/l
              个文件会被替换掉,大小一样
iptablesupdate 存在计划任务,免密登录,常见文件/etc/iptablesupdate,/usr/bin/dockerlogger,
              /etc/init.d/dockerlogger,/tmp/newabchello,进程dockerlogger,iptablesupdate,
              后门账号logger,system,autoupdater,sysall
javaupdateminer XMR挖矿家族,恶意文件/var/tmp/.Javadoc/JavaUpdate,/var/tmp/.Javadoc
              /config.json,/var/tmp/.system-python3.8-Updates,进程名mysqlserver,
              计划任务关键词python3.8m.sh
lh-miner     kingsing家族挖矿,存在库文件劫持,后门服务bot,常见文件/etc/libsystem.so,
              /etc/kinsing,/etc/kdevtmpfsi,/usr/local/bin/curl,/root/curl,进程kingsing
moneroocean  teamtnt家族,创建服务SystemRaid,常见文件/tmp/.tntcurl,/root/bioset,
              /root/.configure,进程bioset,docker镜像传播 alpinos/dockerapid
ozmminer     缺省注释
powerghost   驱动人生家族变种,/lib/libudev.so,/etc/init.d/markdown,/etc/cron
              .hourly/gcc.sh,/bin/.securetty/.esd-644/markdown,进程名abrtid
pwndns-1     Tsunami僵尸网络病毒家族的一个变种, 部分后门程序更换名字,
pwndns       Tsunami僵尸网络病毒家族的一个变种,主要通信pw.pwndns.pw域名,常见工作目录
              /var/tmp,/bin/下生成恶意文件,服务名pwnrig
SHC-Miner    网络连接进程zapppp,koko,写入免密登陆密钥,常见文件/usr/sbin/070ABnndmg,
              cat /var/tmp/.changed,/home/shindei
SMBGhost     驱动人生家族,/X11/xr/,主要访问域名jue82h.com,u78wjdu.com,qq7u0.com,
              phu7t.com,bb3u9.com,m7n0y.com,z23r0.com,ackng.com,zer9g.com,jddcjq.top,
              aaymx.com,p.b69kq.com
systemdminer 访问带有tor或onion字符串的域名,存在计划任务,主机执行自删除,进程名字是很长的一段哈希,应用漏洞攻击,
              ssh密钥传播,/tmp/.X11-unix/下存放进程id的文件,
thegov       挖矿家族后门,常见文件/etc/ld.so.preload,/usr/bin/kthreadds,/lib/udev/
              clock,/etc/cron.d/0clock,/usr/include/.sysproc,/bin/initr,通信域名thegov.win
vmwareminer  XMR挖矿病毒,进程crosbow,存在库文件劫持,创建目录/usr/local/bbbb
warmup       工作目录/root/.warmup,创建服务warmup,计划任务关键词somescript,warmup
workminer    网络连接中会发起大量攻击线程,进程为work32/64,运行目录一般在/usr/.work
xms8220      Tsunami僵尸网络病毒家族的一个变种,进程名bashirc,cruner,主要通信c4k-rx0.pwndns.pw
              域名,常见工作目录/tmp,/bin/下生成恶意文件,服务名pwnrig,下载url关键词givemexyz,
              oracleservice
xmssminer    某挖矿家族,存在库文件劫持,常见文件/usr/sbin/.inis,/usr/local/lib/lib.so,
              /usr/bin/.libs,/tmp/.libs,/usr/sbin/.rsyslogds,/usr/sbin/.rsyslogds.sh
xorddos      僵尸网络病毒家族

```

3. 病毒检测，程序中预置了这些病毒的特征，可以一键检测系统中是否存在符合库中特征的病毒。

命令举例：./MMH1.3 -CHECK

```

root@MMH:~# ./MMH1.3 -CHECK
当前程序进程pid: 18578
MMHLog:2022/06/13 17:40:20.150093 [+] Start scan virus in your system.
MMHLog:2022/06/13 17:40:20.180665 [*] Found file: /usr/bin/.sshd
MMHLog:2022/06/13 17:40:20.198665 [+] Find some file of gates
MMHLog:2022/06/13 17:40:20.199135 [+] Miners check finish
root@MMH:~# |

```

4. 单个病毒家族扫描，扫描已知家族病毒特征，如下扫描“gates”病毒家族

命令举例：./MMH1.3 -check gates

```

root@MMH:~# ./MMH1.3 -check gates
当前程序进程pid: 18582
[+] Start run POC for gates
MMHLog:2022/06/13 17:40:47.067420
[+] 发现gates病毒特征
root@MMH:~# |

```

5. 病毒一键清除，确定了病毒家族之后就可以加载专杀进行清理了

命令举例：./MMH1.3 -clean gates [-CLEAN] 加载库中所有的专杀模块，相对较慢

```

root@MMH:~# ./MMH1.3 -clean gates
当前程序进程pid: 18595
[+] Start run EXP for {gates}
MMHLog:2022/06/13 17:41:28.549016
[+] clean file --> /usr/bin/.sshd
[-] Scan process.Can't find process named like /usr/bin/.sshd
[+] Clean Finish

[+] 为避免正常文件被错杀，请手工检查以下命令是否被替换，查看大小,可直接复制命令执行
[+] Check your command in system
ls -l /usr/bin/ps
ls -l /usr/bin/netstat
ls -l /usr/sbin/ss
ls -l /usr/sbin/lsof
[+] 被替换的文件大小大约为 1223123，如果以上四个文件大小一致，代表被替换过。
[+] 原文文件做了备份，在目录/usr/bin/dpkgd 下，请手动删除病毒文件后还原。
[+] 在确保命令被替换 和 备份命令存在的情况下，可使用下面的命令还原
[+] recover your command,pls exec command here.
rm -f /usr/bin/ps && cp /usr/bin/dpkgd/ps /usr/bin/ps
rm -f /usr/bin/netstat && cp /usr/bin/dpkgd/netstat /usr/bin/netstat
rm -f /usr/sbin/ss && cp /usr/bin/dpkgd/ss /usr/sbin/ss
rm -f /usr/sbin/lsof && cp /usr/bin/dpkgd/lsof /usr/sbin/lsof

root@MMH:~# |

```

6. 进程名检测，MMH1.3可以通过扫描进程，识别库中预置的常见病毒进程名，把可疑的进程列出来。

命令举例：./MMH1.3 -PROC

```
root@MMH:~# ./MMH1.3 -PROC
当前程序进程pid: 18869
MMHLog:2022/06/13 17:42:43.921613 [+] 扫描出的进程仅供参考，可疑进程请再次确认。
MMHLog:2022/06/13 17:42:43.921831 [+] Start scan process.
MMHLog:2022/06/13 17:42:43.959543
root      1453    0.0   0.7 11233552 59000 pts/2    Sl+   6月12   0:02 /root/.local/share/JetBrains/
root      18638   3.0   0.2 911464 18728 ?        Ssl   17:42   0:00 /opt/work32 -daemon

MMHLog:2022/06/13 17:42:43.960150 [+] Scan END!
root@MMH:~#
```

7. 计划任务检测，MMH1.3扫描cron计划任务的日志，以识别是否存在可疑的计划任务。

命令举例：./MMH1.3 -cron

```
root@MMH:~# ./MMH1.3 -cron
当前程序进程pid: 18980
MMHLog:2022/06/13 17:45:10.559359
/var/spool/cron/crontabs/zhj
/var/spool/cron/crontabs/root
/var/log/cron starting udev.sh
/var/log/cron (root) CMD (/usr/share/clamav/freshclam-sleep > /dev/null)
/var/log/cron finished udev.sh
/var/log/cron-20220109 starting udev.sh
/var/log/cron-20220109 (root) CMD (/usr/share/clamav/freshclam-sleep > /dev/null)
/var/log/cron-20220109 finished udev.sh
/var/log/cron-20220102 starting udev.sh
/var/log/cron-20220102 (root) CMD (/usr/share/clamav/freshclam-sleep > /dev/null)
/var/log/cron-20220102 finished udev.sh
/var/log/cron-20211226 starting udev.sh
/var/log/cron-20211226 (root) CMD (/usr/share/clamav/freshclam-sleep > /dev/null)
/var/log/cron-20211226 finished udev.sh
/var/log/cron-20211220 starting udev.sh
/var/log/cron-20211220 (root) CMD (/usr/share/clamav/freshclam-sleep > /dev/null)
/var/log/cron-20211220 finished udev.sh
/etc/cron.weekly/man-db
/etc/cron.d/anacron
/etc/cron.daily/popularity-contest
/etc/cron.daily/man-db
/etc/cron.daily/dpkg
/etc/cron.daily/bsdmainutils
/etc/cron.daily/apt-compat

MMHLog:2022/06/13 17:45:10.563106
* * * * echo htget123 > /tmp/1.sh

root@MMH:~#
```

8. 使用Yara扫描进程,使用yara需要自己准备规则文件如rule.yara，灵活编写规则让扫描更准确便捷。

生成yara规则模板

命令举例：./MMH1.3 -init 会在当前目录创建simple.yara文件

```
root@MMH:~# ./MMH1.3 -init
当前程序进程pid: 25865
rule RuleName
{
    meta:
        description = "This is simple"
        threat_level = 4
        in_the_wild = true
        //https://blog.csdn.net/lisasue/article/details/52457429
    strings:
        $my_text_string = "text here" nocase //nocase不区分大小写
        $my_hex_string = {E2 34 A1 C8 23 FB}
        $wide_string = "Borland" wide //宽字符
        $wide_and_ascii_string = "Borland" wide ascii //宽字符，也想表示ASCII码
        $text_fullword_string = "foobar" fullword //单个词组文本字符串
    condition:
        $my_text_string or $my_hex_string or $wide_string and filesize > 200KB
}
```

```
MMHLog:2022/06/13 17:59:32.150433 simple.yara规则模板创建完毕!
root@MMH:~#
```

9. 进程检测，使用自定义规则扫描进程

命令举例: `./MMH1.3 -rule yara.yar -pid [pid]`

```
root@MMH:~# ./MMH1.3 -rule /opt/rules.yara -pid 19097
当前程序进程pid: 19254
MMHLog:2022/06/13 17:51:32.075552 PID: 19097, Matches: oldfox_yara
Spend Time: 11.110508ms
root@MMH:~#
```

10. Yara扫描所有系统进程

命令举例: `./MMH1.3 -rule yara.yar -PIDS`

```
MMHLog:2022/06/13 17:49:40.337508 Thread: 1, Scanpid: 19097
MMHLog:2022/06/13 17:49:40.398840 PID: 19097, Matches: oldfox_yara
MMHLog:2022/06/13 17:49:40.401064 PID: 19097, Matches: wget
MMHLog:2022/06/13 17:49:40.401408 Thread: 1, Scanpid: 19156
MMHLog:2022/06/13 17:49:40.401611 Thread: 1, Scanpid: 19156
MMHLog:2022/06/13 17:49:40.401805 could not attach to process
MMHLog:2022/06/13 17:49:40.401962 Thread: 1, Scanpid: 19163
MMHLog:2022/06/13 17:49:40.402147 Thread: 1, Scanpid: 19163
```

扫描结果会显示命中的进程号和规则名称, 如上图命中的PID 19097和规则名oldfox_yara, 是apt家族“老狐狸”的病毒。

11. 文件扫描, Yara扫描文件

命令举例: `./MMH1.3 -rule yara.yar -f filename`

```
root@MMH:~# ./MMH1.3 -rule /opt/rules.yara -f /opt/oood
当前程序进程pid: 19273
MMHLog:2022/06/13 17:52:07.415601 filepath: /opt/oood, Matches: oldfox_yara
Spend Time: 3.864862ms
root@MMH:~#
```

12. Yara扫描目录

命令举例: `./MMH1.3 -rule -d`

```
root@MMH:~# ./MMH1.3 -rule /opt/rules.yara -d /opt/
当前程序进程pid: 19281
MMHLog:2022/06/13 17:52:56.265021 into YaraScanDir
MMHLog:2022/06/13 17:52:56.300875 FileName: /opt/oood, Matches: oldfox_yara
MMHLog:2022/06/13 17:52:56.301251 FileName: /opt/callback/godzilla.jsp, Matches: webshell_godzilla
MMHLog:2022/06/13 17:52:56.301345 FileName: /opt/callback/oldfox_stopper.bak, Matches: oldfox_yara
MMHLog:2022/06/13 17:52:56.310695 FileName: /opt/godzilla.jsp, Matches: webshell_godzilla
MMHLog:2022/06/13 17:52:56.311426 FileName: /opt/oldfox_stopper.bak, Matches: oldfox_yara
MMHLog:2022/06/13 17:52:56.345041 Spend Time: 80.015746ms
Spend Time: 80.371156ms
root@MMH:~#
```

13. 显示当前系统进程中的运行程序文件路径

命令举例: `./MMH1.3 -psfile`

```
root@MMH:~# ./MMH1.3 -psfile |tail
PID:21882 user:root path:/opt/oood
PID:21887 user:root path:/root/MMH1.3
PID:21888 user:root path:/usr/bin/tail
PID:21889 user:root path:/root/MMH1.3
PID:21890 user:root path:/root/MMH1.3
PID:21891 user:root path:/root/MMH1.3
PID:21892 user:root path:/root/MMH1.3
PID:21893 user:root path:/usr/bin/bash
PID:21896 user:root path:/usr/bin/bash
```

14. 检测可能隐藏的系统进程

命令举例: `./MMH1.3 -unhide`

```
root@MMH:~# ./MMH1.3 -unhide |tail
PID:18040 user:root path:/usr/libexec/fwupd/fwupd
PID:18041 user:root path:/usr/libexec/fwupd/fwupd
PID:18050 user:root path:/usr/libexec/fwupd/fwupd
PID:19092 user:root path:/usr/local/GoLand-2021.2/jbr/bin/java
PID:19183 user:root path:/usr/local/GoLand-2021.2/jbr/bin/java
PID:24483 user:root path:/root/MMH1.3
PID:24484 user:root path:/root/MMH1.3
PID:24485 user:root path:/root/MMH1.3
PID:24486 user:root path:/root/MMH1.3
```

对本工具有任何疑问和建议，请联系深信服安全服务应急响应中心！