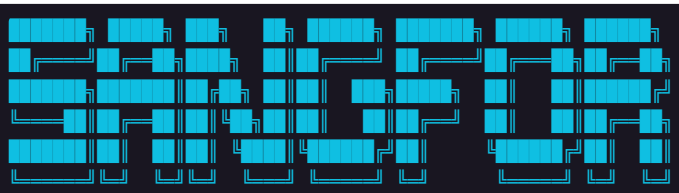
MMH(M78 Miner Helper)使用手册

文件名：MMH1.4（M78 Miner Helper）
版本：V1.4
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



```
#MMH--M78 Miner Helper . (C) 2021-2022 Sangfor_M78_In_ChangSha
Version:1.4
Options:
  -CHECK
        加载所有病毒模块扫描
  -CLEAN
        执行全部专杀模块
  -PIDS
        对系统全部进程进行yara扫描
  -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
  -check string
        检测主机是否存在指定类型的病毒
  -clean string
        对指定的病毒类型一键查杀
  -cron
        分析任务日志以快速定位可疑的计划任务
  -d string
        对指定目录下的文件进行yara扫描
  -f string
        对指定文件进行yara扫描
  -h    查看帮助
  -list
        列出当前支持检测查杀的病毒家族
  -m    生成yara模板
  -pid int
        对系统进程pid进行yara扫描
  -psfile
        显示当前系统进程中的运行程序文件路径
  -rule string
        yara扫描,使用参数指定类型扫描 (default "simple.yara")
  -show
        显示常见病毒的特征表述
  -unhide
        检测可能隐藏的系统进程，仅作参考
Example:
        MMH1.4 -m 生成yara模板
        MMH1.4 -rule /tmp/yara.yar -d /opt/ #yara扫描目录
        MMH1.4 -rule /tmp/yara.yar -f /opt/virusfile #yara扫描文件
        MMH1.4 -rule /tmp/yara.yar -pid pid #yara扫描单个进程
        MMH1.4 -rule /tmp/yara.yar -PIDS #yara扫描全部进程
```

1. 支持查杀的病毒家族
   命令举例：./MMH -list 显示支持的病毒家族

```
root@MMH:~# ./MMH1.4 -list
当前MMH程序进程pid:  3569
MMHLog:2023/03/14 14:48:52.881144 当前支持的专杀有:
                1337Miner
```

```
                automominer
                cleanfda
                Dofloo
                fullskystar
                gates
                iptablesupdate
                javaupdateminer
                kerberods
                kinsing
                lh-miner
                moneroocean
                Outlaw
                oznminer
                pkesi
                powerghost
                pwndns-1
                pwndns
                SHC-Miner
                SMBGhost
                sugona
                systemdminer
                thegov
                Tsunami-kwk
                uninstall
                vmwareminer
                wach
                wannamine
                warmup2
                warmup
                workminer
                xmrig
                xms8220
                xmssminer
                xorddos2
                xorddos
```

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：./MMH -show

```
root@MMH:~# ./MMH1.4 -show
当前MMH程序进程pid:  3579
    1337Miner       ssh传播,meinkampfeth挖矿进程,brute,find.sh,passmaker,ps,zankyo.tar
    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/zzhs,/etc/etc
    Dofloo          僵尸网络家族,写入开机启动项作为持久化,/etc/rc*/rc.local,病毒进程名不定
    fullskystar     云铲挖矿,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几
                    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
    kerberods       一个老牌的挖矿病毒，存在后门服务netdns,kerberods,kthrotlds,kpsmouseds，库文件劫持
    kinsing         别名serv-hello,hezb挖矿;存在kik进程,kinsing,kdevtmpfsi,bot服务,cf.sh
    lh-miner        kingsing家族挖矿,或叫h2miner,guardminer,存在坤文件劫持,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
    Outlaw          僵尸网络家族,.configrc,.rsync,.bashtemp,kswapd0,dota.tar.gz,附加免密登陆,常见a/b/c目录
    oznminer        常见进程名 ./ver ./ozn,edoeprost,sloboz,systemclientupdate,ofshaservice,oMgcdservice
                    存在隐藏账号,存在.a或.x目录存在计划任务,内网代理矿池,查看网络连接很容易识别
    pkesi           2023新兴挖矿病毒，常见/usr/zip，进程pkesi，watchyou脚本
    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abrtd
    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/O70ABnndmg,
                  cat /var/tmp/.changed,/home/shindei
    SMBGhost      驱动人生家族,/.Xll/xr,主要访问域名jue82h.com,u78wjdu.com,qq7u0.com,
                  phu7t.com,bb3u9.com,m7n0y.com,zz3r0.com,ackng.com,zer9g.com,jdjdcjq.top,
                  amynx.com,p.b69kq.com
    sugona        挖矿目录/usr/local/games/.cache,kernel.service后门服务
    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
    Tsunami-kwk   Tsunami家族挖矿病毒，路径/usr/share/man/man1/kwk，/var/local/.x，/etc/init.d/network-man
    uninstall     去除恶意的卸载任务
    vmwareminer   XMR挖矿病毒,进程crosbow,存在库文件劫持,创建目录/usr/local/bbbb
    wach          一个cpu占据高的挖矿，引起宕机，计划任务.mysql/update，/var/.cache
    wannamine     2019年比较活跃的挖矿家族,跨平台,存在diskmanagerd服务和进程,计划任务运行gcc4lef.sh
    warmup2       warmup家族新变种,libgcc_a,crtend_b,pkit.so
    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
    xmrig         门罗币挖矿病毒，默认进程查杀
    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/libs.so,
                  /usr/bin/.libs,/tmp/.libs,/usr/sbin/.rsyslogds,/usr/sbin/.rsyslogds.sh
    xorddos2      僵尸网络病毒家族，pmapx_start_2.service，route_forbidden-close，rmt_remount-open，用户.syslog
    xorddos       僵尸网络病毒家族
```

1. 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：./MMH -CHECK

```
root@MMH:~# ./MMH1.4 -CHECK
当前MMH程序进程pid:  3736
MMHLog:2023/03/14 14:55:38.772331 [+] Start scan virus in your system.
MMHLog:2023/03/14 14:55:38.772780       [*] Found file: /usr/bin/.sshd
MMHLog:2023/03/14 14:55:38.772984       [*] Found file: /usr/bin/bsd-port/getty
MMHLog:2023/03/14 14:55:38.773059       [*] Found file: /etc/init.d/DbSecuritySpt
MMHLog:2023/03/14 14:55:38.773150       [*] Found file: /etc/init.d/selinux
MMHLog:2023/03/14 14:55:38.773274 [+] Find some file of gates
MMHLog:2023/03/14 14:55:38.773425 [+] Miners check finish
```

1. 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：./MMH -check gates

```
root@MMH:~# ./MMH1.4 -check gates
当前MMH程序进程pid:  3755
[+] Start run POC for gates
MMHLog:2023/03/14 14:56:06.497352 [+] 发现gates病毒特征
```

1. 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：./MMH -clean gates [-CLEAN] 加载库中所有的专杀模块，相对较慢]

```
root@MMH:~# ./MMH1.4 -clean gates
当前MMH程序进程pid:  3770
[+] Start run EXP for {gates}
MMHLog:2023/03/14 14:58:49.323757
[+] clean file --> /tmp/gates.lod
[+] kill file --> /tmp/gates.lod
[+] clean file --> /usr/bin/bsd-port/getty.lock
[+] kill file --> /usr/bin/bsd-port/getty.lock
[+] clean file --> /usr/bin/.sshd
[-] Scan process.Can't find process named like /usr/bin/.sshd
[+] clean file --> /usr/bin/bsd-port/getty
[+] clean file --> /etc/init.d/DbSecuritySpt
```

```
[+] clean file --> /etc/init.d/selinux
[+] 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
```

1. 进程名检测，MMH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：./MMH -PROC

```
root@MMH:~# ./MMH1.4 -PROC
当前MMH程序进程pid:  4000
MMHLog:2023/03/14 14:59:56.228235 [+] 扫描出的进程仅供参考，可疑进程请再次确认。
MMHLog:2023/03/14 14:59:56.228859 [+] Start scan process.
MMHLog:2023/03/14 14:59:56.257908
root        3965  0.0  0.0   9732   976 ?        Ssl  14:59   0:00 /usr/bin/.sshd

MMHLog:2023/03/14 14:59:56.259132 [+] Scan END!
```

1. 计划任务检测，MMH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：./MMH -cron

```
root@MMH:~# ./MMH1.4 -cron
当前MMH程序进程pid:  4015
MMHLog:2023/03/14 15:00:53.870794
/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
/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:2023/03/14 15:00:53.871906
* * * * * echo htget123 > /tmp/1.sh
```

1. 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：./MMH -m 会在当前目录创建simple.yara文件

```
root@MMH:~# ./MMH1.4 -m
当前MMH程序进程pid:  4140
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:2023/03/14 15:01:45.901711 simple.yara规则模板创建完毕!
```

1. 进程检测，使用自定义规则扫描进程
   命令举例：./MMH -rule simple.yara -pid [pid]

```
root@MMH:~# cat simple.yara
rule OldFox
{
    meta:
        description = "This is simple"
        threat_level = 4
        in_the_wild = true
    strings:
        $my_text_string = "sbweb.com" nocase //nocase不区分大小写
    condition:
        $my_text_string
}


root@MMH:~# ./MMH1.4 -rule simple.yara -pid 4150
当前MMH程序进程pid:  4304
MMHLog:2023/03/14 15:07:41.493485 PID: 4150, Executable path: /opt/oldfox_stopper.bak, Matches: OldFox
```

1. Yara扫描所有系统进程
   命令举例：./MMH -rule yara.yar -PIDS

```
root@MMH:~# ./MMH1.4 -rule simple.yara -PIDS
当前MMH程序进程pid:  4324
MMHLog:2023/03/14 15:09:02.790747 into YaraScanPids
MMHLog:2023/03/14 15:09:10.877955 PID: 526, Executable path: /usr/lib/systemd/systemd-resolved, Matches: OldFox
MMHLog:2023/03/14 15:11:08.695066 PID: 1395, Executable path: /usr/bin/bash, Matches: OldFox
MMHLog:2023/03/14 15:11:10.895308 PID: 3477, Executable path: /usr/sbin/sshd, Matches: OldFox
MMHLog:2023/03/14 15:11:14.518164 PID: 4150, Executable path: /opt/oldfox_stopper.bak, Matches: OldFox
MMHLog:2023/03/14 15:11:16.474200 PID: 3532, Executable path: /usr/bin/bash, Matches: OldFox
MMHLog:2023/03/14 15:12:04.355521 Spend Time: 3m1.564767223s
```

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 4150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：./MMH -rule yara.yar -f filename

```
root@MMH:~# ./MMH1.4 -rule simple.yara -f /opt/oldfox_stopper.bak
当前MMH程序进程pid:  4372
MMHLog:2023/03/14 15:12:51.092730 filepath: /opt/oldfox_stopper.bak,    Matches: OldFox
```

1. Yara扫描目录
   命令举例：./MMH -rule -d < dir >

```
root@MMH:~# ./MMH1.4 -rule simple.yara -d /opt/
当前MMH程序进程pid:  4383
MMHLog:2023/03/14 15:13:31.941775 into YaraScanDir
MMHLog:2023/03/14 15:13:31.976838 FileName: /opt/oood,  Matches: OldFox
MMHLog:2023/03/14 15:13:31.980481 FileName: /opt/callback/oldfox_stopper.bak,   Matches: OldFox
MMHLog:2023/03/14 15:13:31.993810 FileName: /opt/oldfox_stopper.bak,    Matches: OldFox
MMHLog:2023/03/14 15:13:32.006833 Spend Time: 65.044614ms
```

1. 显示当前系统进程中的运行程序文件路径
   命令举例：./MMH -psfile

```
root@MMH:~# ./MMH1.4 -psfile
PID:3999 user:root path:/home/zhj/GolandProjects/awesomeProject/gates
PID:4150 user:root path:/opt/oldfox_stopper.bak
PID:4349 user:root path:/usr/local/GoLand-2021.2/jbr/bin/java
PID:4397 user:root path:/root/MMH1.4
PID:4398 user:root path:/root/MMH1.4
PID:4399 user:root path:/root/MMH1.4
PID:4400 user:root path:/root/MMH1.4
PID:4401 user:root path:/root/MMH1.4
```

1. 检测可能隐藏的系统进程
   命令举例：./MMH -unhide 该项需要结合人工判断

```
root@MMH:~# ./MMH1.4 -unhide
当前MMH程序进程pid:  5698
MMHLog:2023/03/14 15:15:45.849238
PID:385 user:root path:/usr/bin/vmware-vmblock-fuse
PID:386 user:root path:/usr/bin/vmware-vmblock-fuse
PID:600 user:root path:/usr/lib/accountsservice/accounts-daemon
PID:601 user:root path:/usr/lib/policykit-1/polkitd
PID:602 user:root path:/usr/libexec/switcheroo-control
PID:609 user:root path:/usr/lib/udisks2/udisksd
PID:611 user:root path:/usr/sbin/rsyslogd
```

程序运行发生的日志记录在当前目录的MMH.log文件中

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！